HACKER JOURNAL

Anno 2 – N. 29
3 Luglio - 17 Luglio 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it,

Contributors: Antonino Benfante, Bismark.it, Guglielmo Cancelli, Nicola D'Agostino, DaMe`, Roberto 'dec0der' Enea, Il Coccia, Lidia, Milo Cutty, Gianluca Pomante, SpeedyNT, 3d0.

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Copertina: Zocdesign.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

APERTO È MEGLIO

Qualcuno se l'è presa per un mio articolo di qualche tempo fa, polemicamente intitolato "Usate un fottuto motore di ricerca", nel quale invitavo i lettori a provare a cercare su Internet le informazioni prima di chiederle a noi, e spiegavo come fare. C'è chi si è lamentato del fatto che l'articolo era troppo semplice per una rivista che ha la parola Hacker nel proprio nome, e chi si è offeso per i toni canzonatori.

Ci credereste? Il numero delle richieste "banali", quelle che si risolvono digitando alcune parole in Google e pescando il primo risultato, sono calate di molto. Segno che l'articolo è servito. Forte di questo successo, ci riprovo.

Lo sfogo del giorno è: usate un fottuto formato di file aperto.

La stragrande maggioranza dei documenti che circolano per email, o che vengono pubblicati sul Web, è in un formato proprietario, di cui spesso non esistono specifiche pubbliche (doc, xls, ppt per citare i più diffusi), e questo è un male per vari motivi, che sono spiegati in dettaglio in un articolo di Richard Stallman (Possiamo mettere fine agli allegati in Word, pubblicato in italiano su http://squat.net/tmc/msg02454.html). Ne riassumo i punti principali.

Un formato proprietario obbliga gli utenti a usare il software proprietario. E con il ritmo con cui escono nuovi programmi, gli utenti sono ingabbiati in un ciclo di continui aggiornamenti, che lo vogliano o no.

Se per lo smanettone, che comunque sa come cavarsela, ricevere un file in formato proprietario è un fastidio, per coloro che stanno valutando se passare o meno al software libero, può essere un grosso freno: hanno paura di non poter più comunicare con gli altri.

Un file di Word, per esempio, può essere anche trenta volte più grande di un file che contiene lo stesso testo, e una ventina di volte più grande di una pagina Html che contiene lo stesso testo, con le stesse formattazioni o tabelle. Perché sprecare tanta banda e, per chi ha un modem, tanti soldi per la trasmissione e la ricezione del file?

Stallman propone di rispondere a chiunque ci invii o ci richieda un documento in formato proprietario, con un messaggio di spiegazione: a partire da questo numero, personalmente farò così.

grand@hackerjournal.it

www.hackerjournal.it

HACKER JOURNAL

Saremo di nuovo in edicola Giovedì 17 luglio !

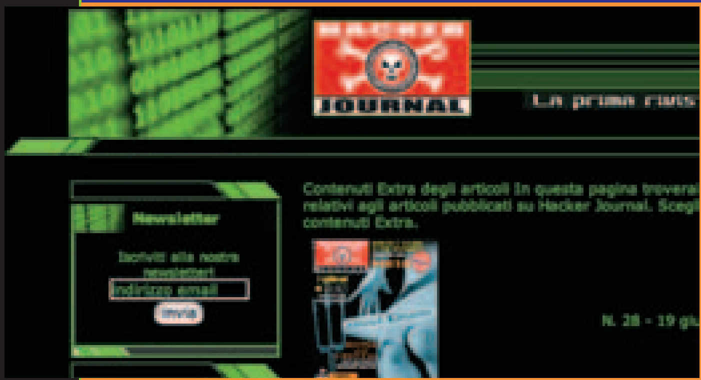
STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Hackerjournal.it, il muro per i tuoi graffiti digitali

w w w . h a c k e r j o u r n a l . i t

I CONTENUTI EXTRA DI HJ



Avete presente i Contenuti Extra dei DVD? Di solito ci sono interviste, scene tagliate, e tutte quelle parti che non possono entrare nel film. Noi abbiamo deciso di fare la stessa cosa, ma con la rivista! Nella Secret Zone (alla quale si accede con la password che trovate in questa pagina), per ogni numero di HJ pubblicheremo una sezione con contenuti aggiuntivi, codici e listati, link, immagini e tutto quello che –per spazio o praticità– non abbiamo potuto stampare sulla carta. Chi vi offre di più?

TRY2HACK RELOADED: LA CLASSIFICA

Ecco i dieci concorrenti che finora hanno superato più livelli nel minor tempo possibile. Pensi di poter fare di meglio: corri su www.hackerjournal.it/try2hackrl e iscriviti al gioco, realizzato in collaborazione con Glesius.it

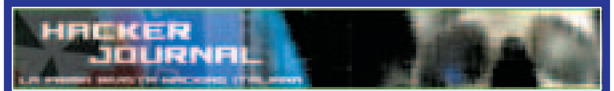
	Nick	Punti
1	Pippo79®	500
2	Soniak	500
3	badpenguin	500
4	Fabio	500
5	|Seto|	500
6	gufino2	500
7	31337	500
8	dos622	500
9	_Axel_	430
10	_mandrake_	420

I NOSTRI/VOSTRI BANNER!

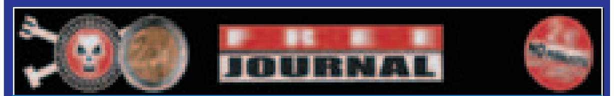
In tanti ci hanno chiesto se avevamo un banner di HJ da pubblicare sul proprio sito. Noi, da bravi paraculi quali siamo, abbiamo ribaltato la richiesta a voi: realizzate un banner per HJ, e noi li pubblicheremo tutti sul sito, e i migliori sulla rivista.



Krakus



Spyro



Sandro



Ufo85

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: tele9la
pass: alpes3

mailto:

redazione@hackerjournal.it

SEGNALARE UNA FALLA

Lavoro come sistemista per una società di informatica, facendo alcuni test con dei portscanner sulla rete di un cliente abbiamo trovato un grosso buco, dopo alcuni controlli abbiamo visto che il problema riguarda tutte le installazioni di un ISP, vorremmo segnalare il problema e farlo risolvere, ma allo stesso tempo non vorremmo rischiare denunce o insabbiamenti da parte del provider, secondo voi qual è la strada migliore?
Per come la penso io , una volta risolto il problema ritengo che questo dovrebbe, per correttezza verso i clienti, essere reso pubblico, ma come fare per evitare che poi il provider neghi tutto facendoci anche fare brutta figura (cosa che mi è già successa)?

Guglielmo S.

Dare la notizia di un bug o di una falla non è un reato in sé. Il problema è che, probabilmente, il reato lo hai compiuto per trovare la falla (se, per esempio, hai ottenuto accesso a un sistema che non possiedi o amministri tu).
Se così non è, rimane il problema morale: diffondere la notizia, lasciando un sistema attaccabile da chiunque, non è una buona idea, non solo per i proprietari del sistema, ma anche per tutte le persone e le aziende che utilizzano il sistema e confidano nella sua sicurezza.
Solitamente, in questi casi, si invia un rapporto sulla falla all'amministratore del sistema in questione, avvisandolo che il rapporto sarà reso pubblico - per esempio - nel giro di un mese. L'azienda ha tutto il tempo di intervenire e correggere il problema, ma ha un chiaro motivo per non ignorare o insabbiare la cosa.

☺ Tech Humor ☺



COMPILATORE BASIC C64

In una lettera che vi è arrivata, e che avete pubblicato sul n27 con titolo "BASIC E C64", avete detto che non esiste un compilatore per il Basic. Falso, esiste! Ai tempi, si parla di all'incirca 15 anni fa, avevo fatto un'applicazione con 8 o 16 sprite (sprite=oggetti che disegnati come una matrice si possono muovere in giro per lo schermo) e interpretato si muoveva a velocita' "lumaca". In seguito su una rivista avevo trovato un programma che mi trasformava il sorgente basic in codice macchina. Dopo aver quindi compilato il mio programmino la velocità era nettamente superiore.
L'unico peccato che essendo passato così tanto tempo non ricordo il nome. Pero' se si chiede su i diversi siti specializzati di C64 forse qualcuno ha ancora quell'applicazione.

Verissimo, hai ragione, anche se la lettrice chiedeva semplicemente come poter cominciare a programmare in Basic, cosa che con il C64 si può fare senza bisogno di compilare i programmi.

DATABASE IMEI

Scrivo in relazione alla notizia apparsa sul numero 27, della vostra rivista, riguardante la creazione di un database unico dei codici IMEI.
Non condivido l'allarmismo riguardo la riduzione della privacy degli utenti. Essa infatti non viene ridotta più di quanto già non lo sia. Già adesso i gestori tengono un database dei codici IMEI e hanno i mezzi tecnici per impedire l'accesso ad un cellulare che risulta rubato. Ciò non è stato fatto finora perché i database erano propri di ogni gestore, di fatti cambiando gestore telefonico si poteva usare il cellulare impuniti.
L'unione dei database determina quindi solo un punto a favore degli utenti. Inoltre esso dovrebbe contenere solo i dati di cellulari rubati, pertanto non si mina alla privacy dei normali utenti. Cerchiamo di non creare allarmismi inutili.

Nessuno vuole creare allarmismi, però è meglio continuare a riflettere su tutte le possibili implicazioni della tecnologia. Anche la più innocente all'apparenza. Nei regimi totalitari, Internet, cellulari e computer sono diventati un mezzo in più per controllare la popolazione. Non dimentichiamolo mai.



Questo pomeriggio non sapevo cosa fare e mi sono sbizzarrito col pirografo e... guardate un po' che cosa sono riuscito a fare! (Gick)

PRIORITA' NEL P2P

Io e un mio amico ci scambiamo i risultati di una tesina tramite P2P (ne abbiamo usati molti). Questi file sono di matlab e pesano pochi kb. Mentre scarico questi documenti però, scarico anche altri file.
Esiste un modo per far si che questi programmi P2P facciano prima e subito il download dei file piccoli, o per lo meno esiste un modo per dare più banda a quei file a cui mancano pochi byte per essere downloadati completamente, rubandola a quelli che si trovano praticamente all'inizio?

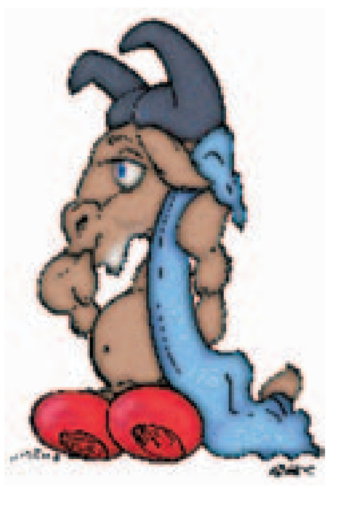
Molto dipende dal programma usato, ma soltanto tutto il controllo sia nelle mani di chi condivide. In pratica, tu potrai far partire immediatamente il download del tuo amico, e lui potrà fare lo stesso con il tuo: basterà solo coordinarvi via chat, e richiedere l'avvio del file che ti interessa ricevere per primo.

RICERCHE AUTOMATICHE

Esiste un programma che date un paio di parole da cercare lui inizia a scaricarsi tutte le pagine Web che il motore di ricerca ha trovato? per farmi capire cosa intendesse mi ha fatto l'esempio di Matrix all'inizio dove Neo sta dormendo e il computer si scarica da solo le informazioni su Morpheus.

Pozzo

Qualcosa di simile si può fare con Copernic, che si scarica da www.copernic.com ed esiste in tre versioni diverse. Per chi fa ricerche molto frequenti, è una vera manna: permette di filtrare e verificare i risultati, e di ordinarli secondo diversi criteri, per trovare più velocemente ciò che si sta cercando.



Molto interessante è anche Google Viewer, una delle modalità "beta" del motore di ricerca, che a intervalli di tempo prefissati, visualizza la pagina corrispondente ai risultati ottenuti dalla ricerca. Lo trovi su http://labs.google.com/gviewer.html (su http://labs.google.com trovi molte altre cose interessanti).

P2P E VIDEOREGISTRATORI

E' vero che negli USA un giudice ha dato ragione alla Sharman Networks (quella di Kazaa) nella causa contro i discografici, adducendo come motivo il diffuso uso della popolazione dei videoregistratori, e che quindi se avesse condannato la Sharman Networks avrebbe dovuto condannare più o meno tutti gli States?

Il fatto è vero, il motivo è un po' diverso. La giuria ha accolto la tesi della difesa, che ha ritirato in ballo una vecchia sentenza del 1984. Ai tempi, l'industria del cinema aveva fatto causa a Sony, che cominciava a vendere i videoregistratori Betamax che potenzialmente potevano essere usati per copiare illegalmente i film. Allora, il tribunale aveva stabilito che - siccome esistevano molti usi legittimi per un videoregistratore - il produttore non poteva essere responsabile degli usi illegali, che andavano addossati solamente agli utenti. Insomma, non si accusa un produttore di piedi di porco di agevolare i furti negli appartamenti. Curiosamente, Sony questa volta si trovava dall'altra parte della barricata (tra i discografici, con la sua Sony Music), ed è stata colpita con le sue stesse armi.

☺ Tech Humor ☺



Creare, non distruggere

Salve a tutta la redazione di Hacker Journal, sono un ragazzo di 20 anni, che ha cominciato da poco a smanettare "seriamente", e dico seriamente perché da qualche mese, dopo 6 anni di computer, ho iniziato a studiare alcuni dei linguaggi di programmazione. Ho letto di come diventare un hacker collegandomi ad un sito che avevate segnalato tempo fa, e mi sono accorto di come non sia solo.
Tempo prima di conoscere questa disciplina "Hacker" (la chiamo così amichevolmente) ero della convinzione che tutto a questo mondo andasse a fondo. La perdita di valori, la mancanza di rispetto, la poca voglia di acculturarsi, di fare...
Adesso un'energia nuova si manifesta, spingendomi a migliorare ogni giorno; sapere che c'è qualcun altro che spinge la conoscenza mi fa apprezzare di più ciò che vivo. Mi dispiace soltanto che molti "Smanettoni", hanno una concezione distorta di ciò che vuol dire HACKER, volti alla distruzione di qualsiasi cosa, questo perché mancano di cultura, altri che invece conoscono e lo fanno comunque probabilmente hanno il cervello frammentato e qualche chiave di registro che non funziona.
Molte volte mi sono chiesto: perché agire in questo modo? Farsi notare? Troppo stupido. Dimostrare di essere i migliori? Così facendo dimostrano solo di non aver rispetto per niente e nessuno. Dovremmo utilizzare la tecnologia per migliorare il mondo, ma come se chi dovrebbe impegnarsi non fa altro che peggiorare le cose.
La tecnologia è sempre stata mascherata con il concetto di bene, mentre dietro hanno sempre fatto in modo che l'effetto fosse opposto. Questo chi lo fa? Chi ha il potere e trae energia e ricchezza dalle condizioni di ignoranza, di vita del popolo. Non credete che tutto questo ben di dio tecnologico abbia cambiato le cose, perché hanno permesso di farci possedere l'impianto elettrico, i termosifoni, le automobili allo scopo di migliorare le nostre condizioni, ma per far in modo di poterci fruttare meglio.
La verità a mio parere è una: se vogliamo migliorare il mondo dobbiamo prima migliorare noi stessi, cominciando a finirla col distruggere le cose ma riparare quelle danneggiate.
Respect and hacking

=Jhonny.zelawsky=

NEWS

NUMERI

PRESO IL CRACKER DI AL JAZEERA



Nei giorni della guerra in Iraq, un cracker americano patriottico aveva dirottato su un diverso server le connessioni indirizzate al sito dell'emittente televisiva Al Jazeera. A suo tempo, noi avevamo ipotizzato l'utilizzo di una tecnica chiamata DNS Poisoning, e l'avevamo descritta sul n. 24. In realtà, l'autore del fattaccio, ha utilizzato una tecnica più rudimentale ma non meno efficace: falsificando fax della TV, è riuscito a farsi dare da Network Solutions la password per modificare i dati del server DNS. Ora rischia fino a 25 anni di carcere, e 500.000 dollari di multa.

L'ULTIMO DEGLI EXPLORER

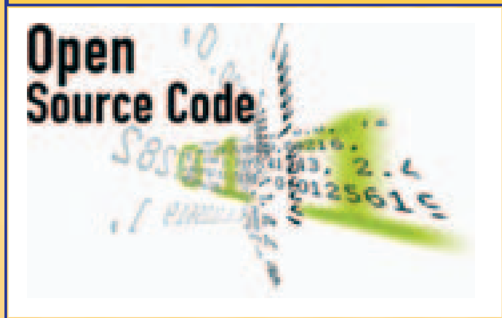
A seguito del rilascio di Safari, browser ufficiale di Apple, e della continua crescita dei browser alternativi per Mac OS X (Chimera e Mozilla sopra tutti), Microsoft ha annunciato di non avere più intenzione di creare nuove versioni di Internet Explorer per i computer della mela. Continuerà invece ad aggiornare l'esistente, con patch per risolvere bug e problemi di sicurezza. Tutt'altro che affranti, gli utenti Mac si stanno ancora chiedendo se si tratta di una minaccia, o invece di una promessa.

AZZURRA CAMBIA POLICY SUL FILE SHARING



Grazie anche alla semplicità con cui si possono registrare nickname e canali usufruendo di molti servizi, Azzurra.org è diventato uno tra i più popolari network Irc in Italia (anche la chat di Hacker Journal è ospitata su Azzurra). Nei giorni scorsi, gli amministratori hanno diffuso ai propri utenti una nota nella quale vietano la creazione di nuovi canali che facciano esplicito riferimento, nel nome o nella descrizione, allo scambio di file. Non sarà vietato lo scambio di file in sé, purché avvenga su canali finalizzati alla discussione, e non sarò chiuso alcun canale registrato prima del 13 giugno. I canali creati successivamente potranno essere chiusi nei primi 90 giorni di vita, a totale discrezione dello staff di Azzurra. Secondo quanto si legge nell'annuncio postato sul forum di Azzurra, "il cambio di policy è dettato dal fatto che la rete negli ultimi tempi sembra molto piu' simile ad un circuito di File Sharing, oltre a questo dobbiamo purtroppo constatare il bassissimo profilo della maggioranza degli utenti che frequentano questo tipo di canali. Si sprecano tra questa classe di utenti le segnalazioni di spam, i dispetti vari, flood e azioni di lamering vario, basti pensare a quanti utenti entrano su #italia, #liberozone, #debian o qualsiasi canale di chat esordendo con il classico !list o @find".

L'OPEN SOURCE CONQUISTA LO STATO



Il Ministero per le Innovazioni e le Tecnologie ha finalmente reso ufficiale la decisione di adottare software open source per la Pubblica Amministrazione. Certo, non si tratta di una scelta radicale, nel senso che di volta in volta le PA potranno scegliere anche altre soluzioni in base alle specifiche esigenze. Ma già così è un grande passo.

I vantaggi di questa politica li possiamo ben immaginare: se ne andranno le pastoie della dipendenza da un singolo fornitore, migliorerà l'accessibilità per le piccole realtà di sviluppo, e ci saranno maggiori garanzie di sicurezza. Infine, tutto ciò costituirà un sostanziosissimo risparmio per le casse dello Stato. A occhio e croce, si potrebbero risparmiare intorno ai cento milioni di Euro all'anno sui costi delle licenze. Che per come vanno i bilanci pubblici, non è niente male.

È UN MAC IL PC PIÙ VELOCE AL MONDO

Nel corso della conferenza per sviluppatori Apple WWDC, Steve Jobs ha presentato il nuovo Mac OS 10.3 Panther, che sarà disponibile a fine anno, e la nuova generazione di Power Macintosh, che invece toccherà gli scaffali già in agosto. Proprio questi ultimi prodotti hanno suscitato il maggiore scalpore; Apple ha infatti abbandonato i processori Motorola in favore dei nuovi PPC IBM 970 con architettura a 64 bit. Per non strozzare il collo ai nuovi processori G5, Apple ha ridisegnato l'intera scheda madre, aumentando la larghezza di banda di praticamente ogni bus, dalla memoria RAM ai dischi fissi. Una curiosità: nei giorni precedenti alla conferenza, le specifiche dei nuovi G5 sono state pubblicate per errore sul sito di Apple. Sapendo quanto Steve Jobs ami stupire il pubblico dal suo palco, non vogliamo immaginare cosa può essere successo al maldestro Webmaster…



NEMICI DI LINUX ALLO SCOPERTO



Da qualche tempo Santa Cruz Operations (SCO) sta accusando la comunità Linux (e IBM in particolare) di utilizzare parti di codice Unix, di cui detiene i diritti di sfruttamento. Fino a un paio di settimane fa, sembrava una piccola scaramuccia legale, che si sarebbe conclusa con un indennizzo di pochi milioni di dollari, tarallucci e vino. E invece SCO ha rincarato la dose: ha revocato a IBM la licenza di Unix, e ha dichiarato pubblicamente che tutti gli attuali possessori di un sistema IBM/AIX devono distruggere la loro copia di Linux. IBM ha replicato che la propria licenza di Unix è, per contratto, perpetua e irrevocabile, e ha rassicurato i suoi clienti, che preoccupati lo sono davvero. Anche perché non si sta parlando di qualche serverino che può essere facilmente sostituito con un altro, ma di complicatissimi sistemi di gestione di multinazionali del calibro di Colgate, di strumenti per il servizio meteorologico degli USA, o di quelli che gestiscono la sicurezza dell'arsenale nucleare USA.

GUERRA DI SLOGAN





In attesa che la vicenda arrivi nelle aule giudiziarie, gli utenti Linux già si stanno facendo sentire: a metà giugno è stata organizzata una protesta davanti alla sede di SCO, la cui risposta è stata quanto mai bizzarra e subdola. Invece di reagire a muso duro, i dipendenti di SCO sono scesi per strada insieme ai manifestanti, mostrando però cartelli poco ortodossi, nei quali per esempio il pinguino Tux affermava "Io amo la pirateria software", oppure "Se ti piace il comunismo, installa Linux". La cosa triste, è che i manifestanti "originali" hanno lasciato fare, e si sono fatti fotografare accanto ai protestatori farlocchi, coi cartelli falsi.

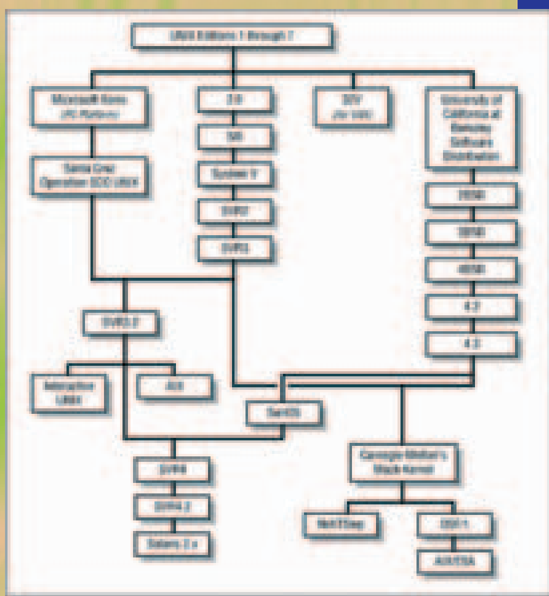
PATTO CON IL DIAVOLETTO

Un po' più seri sono invece quelli che stanno spulciando il codice Linux alla ricerca di possibili parti incriminate, per smontare le accuse di SCO. Tra di essi, qualcuno sta anche azzardando un'ipotesi. Linux e l'attuale Unix di SCO potrebbero avere parti di codice in comune per un motivo molto semplice: entrambe hanno "pescato" a piene mani dal codice sorgente di BSD, operazione pienamente legittima secondo i termini della licenza BSD. Se così fosse, SCO non potrebbe rivendicare la paternità di quelle sezioni del kernel.



RELAZIONI IN FAMIGLIA

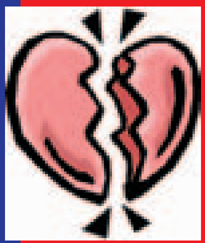
Un altro filone di difesa riguarda il fatto che, negli USA, affinché un'azienda possa rivendicare diritti sui propri brevetti, deve dimostrare di aver sempre fatto di tutto per tutelare al massimo i suoi segreti industriali. Negli scorsi anni, SCO aveva rivelato il codice sorgente di Unix con speciali licenze per le università e gli studenti; queste licenze prevedevano un obbligo di riservatezza, e vietavano l'utilizzo del codice in altri programmi o sistemi. Sembra però che svariate persone siano riuscite ad avere accesso a questo codice, in modo legittimo, senza dover firmare alcun contratto. In questo caso, le rivendicazioni di SCO sarebbero nulle, afferma Eric Raymond, che nei mesi scorsi si era messo proprio alla ricerca di sviluppatori che avessero potuto vedere i sorgenti di Unix senza firmare alcunché. Il tutto però potrà essere stabilito con certezza solo in tribunale. La telenovela, continua.



NEWS

HOT!

IN AMORE TUTTO È CONCESSO



Non ti rassegni al fatto che la fidanzata ti abbia lasciato e vuoi controllarla in ogni suo spostamento e incontrarla "per caso" quante più volte possibile? Semplice: installi un GPS sotto la scocca della sua auto e il resto vien da sé. È quello che ha fatto un innamorato dal cuore infranto nel Wisconsin, Stati Uniti. Un ragazzino? Macché: un maturo quarantatreenne, che, beccato dalla polizia, adesso dovrà scontare nove mesi di galera e cinque anni di libertà vigilata.

I METALLICA CI RIPENSANO

A cambiare idea, soprattutto quando conviene, si è sempre in tempo. Lo dimostrano i Metallica, che dopo aver fatto il diavolo a quattro qualche anno fa contro Napster e la musica distribuita online, ora tornano sulle proprie decisioni dichiarando di voler diffondere mp3 gratis in Rete. Nell'ultimo CD si trovano dei codici che permetteranno all'utente di scaricare tutti i brani dell'abum e anche altri inediti. I fans ringrazieranno riconoscenti. Tutti quelli che si ricordano che Napster è andato al patibolo anche grazie alle battaglie dei Nostri, un po' meno.



PRIGIONE PER CHI CRACCA E DISTRIBUISCE

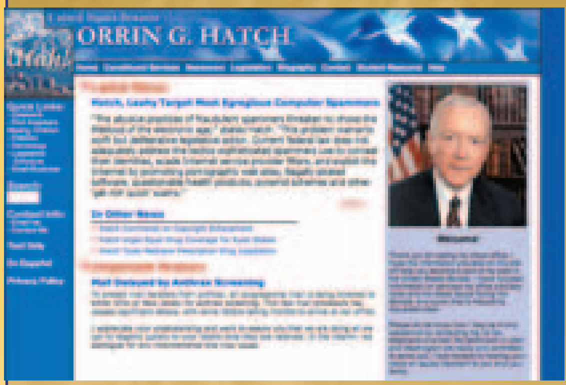
È finito dietro alle sbarre e ci resterà per un anno e mezzo Shane Pitman, responsabile di avere distribuito in Rete centinaia di copie craccate di videogame. Considerato il leader del gruppo Razor 1911, Pitman è stato preso nel corso di una mastodontica operazione di polizia. Al capo di DrinkOrDie, altro colosso della distribuzione pirata, è andata anche peggio: dovrà restare in gattabuia per quattro anni.

DI COSA HANNO PAURA GLI AMERICANI…



Dopo la giustificata paura di un attentato terroristico, sapete qual è la più grande paranoia dell'americano medio? Non la possibilità di un furto in casa, non quella che il partner gli metta in testa una compsosizione di corna da record, non malattie e piaghe di ogni genere. No. La paura del furto di identità su Internet e non. Guerra e virus informatici invece, sono molto indietro nella classifica, tanto da meritarsi solo il 19% e il 6% dei voti. Questo è quanto emerge dai risultati di un'indagine commissionata da RSA Security. Curioso è scoprire che oltre il 40% degli intervistati, gli stessi terrorizzati dai possibili furti di identità, ammette di non avere preso nessuna tra le più elementari norme di sicurezza per proteggersi. Tra loro nessuno ha installato un antivirus come si deve, o si è preoccupato di verificare le politiche di sicurezza adottate dalla propria banca nelle transazioni. Davvero strani questi americani.

L'FBI ATTACCA GLI UTENTI P2P



Negli USA si sta discutendo una legge che permetterà all'FBI, in concerto con le associazioni dei discografici e con il supporto obbligatorio dei provider, di sferrare attacchi informatici contro i computer di chi utilizza software di file sharing. Il tutto senza nemmeno arrivare a un'identificazione, né passare per un tribunale. Il tutto ovviamente sta mettendo in subbuglio i paladini della privacy e dei diritti civili: significherebbe creare una pericolosa situazione in cui i crimini compiuti nel cyberspazio verrebbero giudicati sommariamente, una cosa da "far west". Ancor peggio, l'FBI avrebbe mano libera per colpire anche al di fuori dei confini dello stato, in base al dubbio principio secondo il quale "se si può accedere ai server dagli USA, per noi il reato viene compiuto in casa, e quindi possiamo agire".

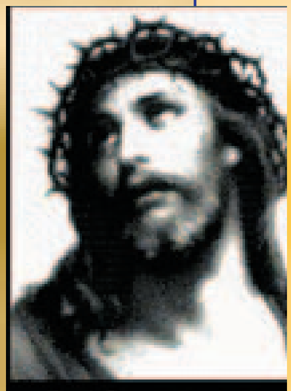
Una nota curiosa a margine: tra i principali sostenitori di questa linea di condotta, c'è il senatore repubblicano Orrin Hatch, che imitando il nostro Ministro per le Riforme, suggeriva di "distruggere i computer di chi scambia musica pirata". Ebbene, da un'analisi del sito Web del senatore effettuata nei giorni della polemica, è risultato che il Webmaster aveva utilizzato un menu in Javascript prodotto dalla software house Milonic Solutions… senza pagarne la licenza! Attento, senatore: se passa la sua stessa legge, l'FBI potrebbe distruggergli il server!

AL MIO COMPUTER MANCA SOLO LA PAROLA

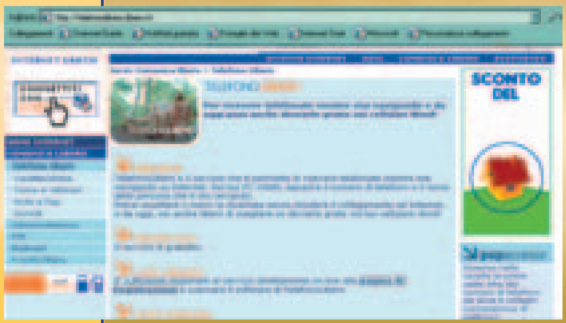


Dopo i concorsi per cani, mucche, veline, velone e miss-ogni-cosa-ogni-luogo, eccone uno riservato ai PC. Si chiama Loebner Prize ed è un concorso di intelligenza per computer che il prossimo ottobre, come ogni anno, assegnerà una bella borsata di dollari alla macchina che più si avvicina a superare il Test di Turing. In cosa consiste il test? Un giudice fa domande e riceve risposte da due diverse postazioni computer lontane dalla sua vista. In una c'è una persona che risponde, nell'altra solo un software di conversazione. Nel momento in cui il giudice non riuscirà a distinguere quali risposte provengono dall'essere umano e quali dalla macchina, ecco che avremo inventato l'intelligenza artificiale. E superato il test a pieni voti.

Ma tranquilli, siamo ancora ben lontani da tutto ciò. Per avere un'idea di come funzionano questi software di conversazione, se ancora non ne abbiamo mai visti, diamo un'occhiata, o meglio facciamo due chiacchiere con Alice (http://www.alicebot.org) , o con Gesù in persona (http://www.crucyfy.com).



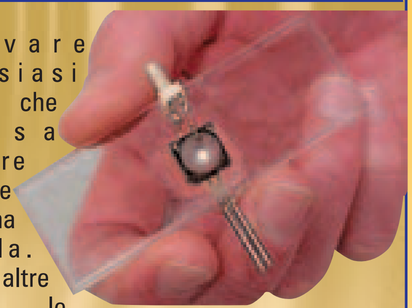
MAI PIÙ OKKUPATI



Chiamare a casa nostra è un impresa. Ormai ci danno per latitanti, stiamo perdendo amici, parenti, fidanzati. Il nostro telefono è perennemente occupato e noi attaccati a Internet come sanguisughe. Se siamo clienti Wind Infostrada oggi c'è un servizio che fa al caso nostro. Con TelefonoLibero possiamo farci avvertire via computer che qualcuno sta provando a chiamarci. Sullo schermo del PC comparirà il numero di telefono o il nome del chiamante. A quel punto potremo decidere se continuare a navigare, se rispondere tramite PC con cuffie e microfono, oppure se deviare la telefonata gratis, per noi e per chi chiama, sul nostro cellulare Wind. TelefonoLibero gestisce infatti solo chiamate in arrivo transitanti su rete Wind. Per usufruire dell'offerta occorre inoltre essere titolare di una casella e-mail Libero o Italia OnLine. Per saperne di più e scaricare il software necessario colleghiamoci a http://telefonolibero.libero.it/

AL SICURO DA ATTACCHI CHIMICI

Centinaia di frequentatori di stadi, sottopassaggi e luoghi a rischio di terrorismo chimico, un giorno potrebbero dover la vita a un chip. Si tratta di un dispositivo messo a punto dall'università di California di Berkeley che contiene un piccola cellula vivente. In caso di attacco chimico, la cellula muore, attivando un allarme acustico. È una sorta di evoluzione tecnologica del metodo usato dai minatori il secolo scorso, che si portavano appresso canarini in gabbia, che morivano alla minima presenza di gas, per rilevare la presenza di sostanze tossiche nelle gallerie. Il sistema è molto meglio di qualsiasi altro attualmente in uso, poiché è in grado di rilevare qualsiasi agente che possa causare la morte di una cellula. Molte altre sono le possibili applicazioni di questo chip. Dalla sicurezza negli ambienti di lavoro, alla verifica della possibile tossicità di alcuni farmaci, per esempio quelli impiegati nella lotta contro il cancro.



LIBRI PER TUTTI

Caldeggiata dall'esponente radicale Pietrosanti e da una commissione di non vedenti, è al vaglio la proposta di vendere su Internet tutti i libri partecipanti al Premio Strega al 6% del loro prezzo di copertina. L'iniziativa intende sensibilizzare l'opinione pubblica e il mondo dell'editoria alle problematiche incontrate dai non vedenti nella fruizione della letteratura. Questa categoria di persone è infatti costretta a svolgere costose e a volte impossibili procedure di scansione delle opere per poterne beneficiare tramite software dedicati. Pietrosanti si appella alla legge sul diritto d'autore che permette ai portatori di handicap di riprodurre materiali protetti da copyright. La proposta sta sollevando un vespaio di polemiche.



HOT!

WEB RADIO IN REGOLA



Finalmente le Radio Americane no profit che trasmettono via Web sono giunte ad un accordo con l'associazione di discografici RIAA. Quest'ultima chiedeva che venissero regolarmente pagati i diritti di trasmissione dei brani musicali. Dopo lunghe discussioni, si è stabilito che per diffondere musica dal proprio sito, le radio dovranno pagare una tassa annuale di 250 dollari se si tratta di radio universitarie, di 400 dollari se si tratta di radio senza finalità commerciali. L'accordo è di tipo retroattivo e dunque per essere perfettamente in regola, le emittenti dovranno pagare gli arretrati a partire dal 1998.

COSÌ GRANDE



"Così grande": suona più o meno così il nome tradotto di uno degli ultimi arrivati nella grande famiglia dei virus informatici. Sobig nelle ultime settimane se ne è andato vagando per le caselle di posta elettronica, recapitando messaggi provenienti, almeno in teoria, niente meno che da Bill Gates. Per fortuna il virus non causa grossi danni: se attivato, si limita a spedire altri messaggi ai contatti della nostra rubrica elettronica.

PORTICINA APERTA ANCHE IN LINUX

Individuata una vulnerabilità di Linux, che se sfruttata potrebbe permettere a un intruso di inviare segnali tipo SIGKILL a processi arbitrari, inclusi quelli di sistema.
I kernel Linux fino alla versione 2.4.18, per intel x86, possono infatti essere forzati a ignorare i privilegi di accesso dell'utente nella gestione di segnali IPC.

CODICE LIBERO, PENSIERO LIBERO

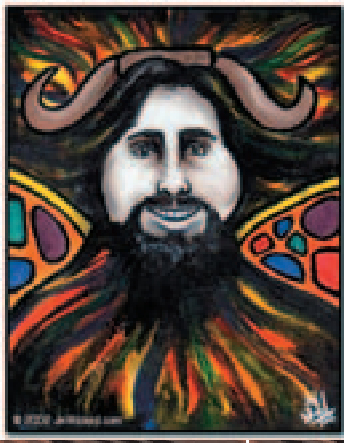
"SE NON POSSO CONDIVIDERLO, ALLORA NON LO USO"

"Esiste un'alternativa al software proprietario e al copyright? Di questi tempi, la domanda è d'obbligo, soprattutto dopo l'entrata in vigore della nuova e più restrittiva normativa sul copyright (l'EUCD), considerata "illiberale" dalle stesse associazioni di consumatori e utenti di Internet! Immaginando di dover rispondere a un lettore poco informato, la risposta è: " Sì, l'alternativa esiste!". Come spiega A. Di Corinto in un suo recente articolo su "Il Manifesto": **"La diffusione di software libero permette oggi di risparmiare sui costi delle licenze di software sotto copyright e di destinarle all'alfabetizzazione di massa alle nuove tecnologie, favorendo altresì il pluralismo informatico e un vero regime di concorrenza fra i produttori di software"** (www.ilmanifesto.it/Quotidiano-archivio/31-Maggio-2003/art84.html).

Per capire i motivi etici che spingono un programmatore a rilasciare software libero basta leggersi **"Software libero, Pensiero libero: Saggi scelti di Richard Stallman"**, a cura di Bernardo Parrella (internet.cybermesa.com/~berny/free.html) e Associazione Software Libero (www.softwarelibero.it), presentato il 15-19 maggio alla Fiera Internazionale del Libro di Torino. Il primo volume (il secondo uscirà in autunno) raccoglie vent'anni di interventi pubblici tenuti da Stallman, e risulta di grande utilità sia per chi non conosce ancora il "Manifesto GNU" e le differenze tra "software libero" e "open source", sia per chi è interessato a temi più complessi, oltre che attualissimi: abusi del copyright, necessità del copyleft e pericoli dei brevetti sul software.

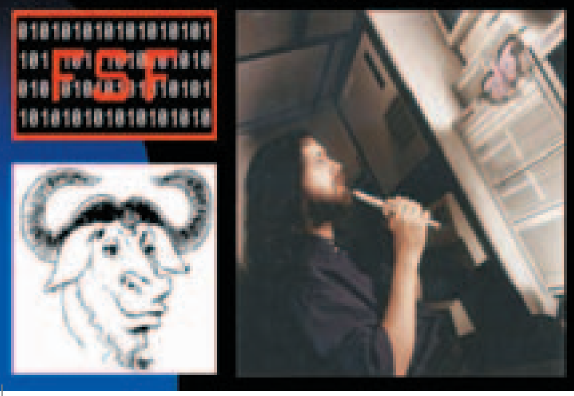
>> Software Libero: la soluzione!

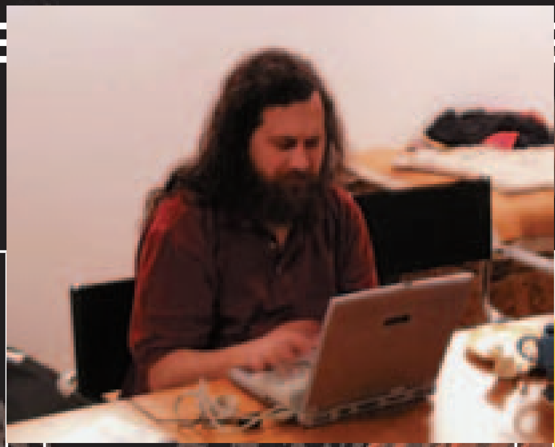
"L'Open Source è una metodologia di sviluppo; il Software Libero è un movimento di carattere sociale. Per il movimento Open Source, il software non libero è una soluzione non ottimale. Per il movimento del Software Libero, il software non libero è un problema sociale e il software libero è la soluzione". (R.M. Stallman)



Stallman (www.stallman.org) sottolinea spesso gli aspetti sociali dell'attività di programmazione e come essa possa creare davvero comunità e giustizia. Libertà e condivisione, ma anche solidarietà e amicizia. Questi i principi che più ricorrono nei suoi scritti, ma anche nella filosofia del "Progetto Gnu" (www.gnu.org) e della "Free Software Foundation" (www.fsf.org) di cui è ideatore. **"Credo che la libertà sia più importante del puro avanzamento tecnico. Sceglierei sempre un programma libero meno aggiornato piuttosto che uno non libero più recente, perché non voglio rinunciare alla libertà personale. La mia regola è, se non posso condividerlo, allora non lo uso."** E' convinto che se un

Richard M. Stallman e la Free Software Foundation





programma piace, debba essere condiviso con altre persone a cui piace.

>> "Free" come Freedom

Il Software Libero è una questione di libertà (free va inteso come "libero", non come "gratuito"), qualcosa di molto simile alla "libertà di parola". Quattro le libertà per gli utenti del software:

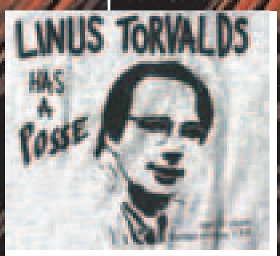


- Libertà di eseguire il programma, per qualsiasi scopo.
- Libertà di studiare come funziona il programma e adattarlo alle proprie necessità (l'accesso al codice sorgente ne è un prerequisito).
- Libertà di ridistribuire copie in modo da aiutare il prossimo.
- Libertà di migliorare il programma e distribuirne pubblicamente i miglioramenti in modo tale che tutta la comunità ne tragga beneficio (l'accesso al codice sorgente ne è un prerequisito).



Un programma può essere considerato Software Libero se l'utente ha tutte queste libertà. Ma affinché si possa essere davvero liberi di fare modifiche e di pubblicare versioni migliorate, si deve avere accesso al codice sorgente del programma.

"Chi usa un calcolatore", afferma Stallman, **"dovrebbe essere libero di modificare i programmi per adattarli alle proprie necessità, ed essere libero di condividere il software, poiché aiutare gli altri è alla base della società".** La condivisione è un atto di amicizia ed è fondamentale tra programmatori. A impedirla, però, le attuali politiche di commercializzazione che, benchè facciano far soldi, costringono inevitabilmente a **"sentirsi in conflitto con gli altri programmatori, invece che solidali".** Stallman si rifiuta di spezzare la solidarietà sia con gli utenti che con gli altri colleghi. **"La mia coscienza, scrive, non mi consente di firmare un accordo per non rivelare informazioni o per una licenza d'uso del software".** E ancora, **"Gli sviluppatori di software proprietario ricorrono al copyright per rubare agli utenti la propria libertà; noi usiamo il copyright per tutelare quella libertà. Ecco perché abbiamo scelto il nome opposto, modificando "copyright" in "copyleft".**



>> Gli utenti prima di tutto!

La licenza Gnu, insomma, rende un programma di pubblico dominio, cioè senza copyright, libero di essere condiviso, modificato e migliorato da chiunque e fa sì che ogni utente conservi queste libertà, senza che qualcuno poco incline alla cooperazione possa un giorno trasformarlo in software proprietario. Permette inoltre ai programmatori di migliorare il software libero, senza che il datore di lavoro, più interessato a trarre gadagni, l'ostacoli.



A ispirare Stallman sono i principi dell'etica hacker, che si è sempre opposta, sin dai tempi del MIT, al diritto di proprietà, ed ha sempre promosso invece la cooperazione, la condivisione del sapere e la libertà di rielaborare e migliorare i prodotti intellettuali altrui. Questi stessi principi e il progetto GNU hanno a loro volta ispirato L. Torvalds che ha realizzato la prima versione del sistema operativo "Linux", messo liberamente in circolazione nel 1991, poi modificato, rielaborato e migliorato da molti programmatori. In conclusione, non si sarebbero realizzate queste ed altre nuove tecnologie, non sarebbe esistita l'informatica come la conosciamo oggi senza questo **"sforzo cooperativo e non remunerato"** di chi **"ha saputo e dovuto agire anche attraverso modalità non sempre ortodosse per riuscire a realizzare ciò che altrimenti la politica, la burocrazia o l'economia non avrebbero reso possibile"** (A. Di Corinto e T.Tozzi, "Hacktivism"). E del resto, volendo spingerci un po' oltre e ricalcando una riflessione di Wu Ming 1, **"se fosse esistita la proprietà intellettuale, l'umanità avrebbe mai conosciuto l'epopea di Gilgamesh, il Mahabharata e il Ramayana, l'Iliade e l'Odissea, il Popol Vuh, la Bibbia e il Corano, le leggende del Graal e del ciclo arturiano, l'Orlando Innamorato e l'Orlando Furioso, Gargantua e Pantagruel"?** (www.informationguerrilla.org/copyright_e_maremoto.htm).



DaMe`

LA RIVOLUZIONE "SENZA FACCIA" DI WU MING

"E' consentita la riproduzione parziale o totale dell'opera e la sua diffusione per via telematica ad uso personale dei lettori, purchè non a scopo commerciale". Tradotto: la diffusione deve rimanere gratuita!
Questa la dicitura dei libri di Wu Ming, un collettivo di agitatori della scrittura (eredi del già famoso Luther Blisset Project) che ha utilizzato il "copyleft" per permettere la libera riproduzione dei propri testi, dimostrando in tal modo come possa essere applicato, con qualche piccola modifica, anche ad un ambito non informatico (www.wumingfoundation.com).



RICETTAZIONE E OPERE DELL'INGEGNO

In qualche procura italiana, c'è chi vorrebbe accusare di ricettazione gli utenti dei software di file sharing. Si tratta di un reato che prevede pene molto severe. E' un'accusa legittima, o forse qualcuno sta davvero esagerando?

Che le multinazionali del software, del cinema e della musica avessero una forte influenza sui governi non era un mistero: ne sono testimonianza evidente le leggi promulgate nel corso degli anni per garantire la tutela dei profitti, moltiplicatesi come funghi e sempre più restrittive, nel nome di un diritto d'autore che sembra sempre più, invece, il classico specchietto per le allodole.

Ma che il bombardamento mediatico garantito da tv e giornali negli ultimi anni fosse in grado di stravolgere elementari principi di diritto, di certo, non se l'aspettava nessuno.

>> Mondo materiale...

Su alcuni punti, le leggi sono molto esplicite: per esempio, la legge sul diritto d'autore garantisce i diritti morali e patrimoniali sulle opere dell'ingegno, distinguendole nettamente dai brevetti industriali per la diversità ideologica che li caratterizza. I processi industriali e le invenzioni hanno infatti una finalità e una caratteristica materiale, mentre la produzione intellettuale è immateriale ed evanescente.

Per questo, negli anni '50, si era tentato di accordare una tutela alle opere dell'ingegno con un artifizio giuridico, secondo il quale le opere erano incorporate e imprigionate nel supporto materiale in modo indivisibile: non si poteva separare l'opera dal disco in vinile o dal libro, e senza disco o senza libro non era possibile godere del beneficio intellettuale derivante dalla loro fruizione.

Per lo stesso motivo, non si soleva distinguere tra tutela accordata al libro in quanto tale e l'opera in esso contenuta giacchè, per esempio, nel furto subìto da un legittimo proprietario, era più che evidente lo spossessamento di entrambi.

>> ...e mondo digitale

A distanza di cinquant'anni, tuttavia, il mondo è cambiato, e con esso il modo di produrre e di godere delle opere dell'ingegno, che sempre più spesso si diffondono nell'etere e su Internet con la stessa fluidità, senza essere più ancorate ad alcun supporto fisico.



La duplicazione digitale ha sostanzialmente reso indistinguibili gli originali dalle copie, e tale trasformazione ha avvicinato i supporti ottici e magnetici molto più al cervello umano che al supporto fisico indispensabile, in passato, per fruire della musica o del cinema.

A tale modifica il mondo giuridico ha reagito in modo deciso, producendo una norma che riporta l'attenzione sull'opera, svincolandola dal supporto. Una parte di questo stesso mondo, pe-

rò, nega questa separazione, continuando a parlare di ricettazione in relazione ai reati tecnologici che hanno ad oggetto le opere dell'ingegno.
L'articolo 648 del Codice Civile definisce appunto il reato di ricettazione, e punisce "chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto". Nel caso della duplicazione abusiva di software, però, non sempre si rinviene il delitto di cui si parla. La duplicazione, infatti, è prevista per effettuare una copia di riserva, e quindi non è un atto punibile in sé.
Anche l'espresso riferimento al profitto, fatto nell'art. 171 bis della legge sul diritto d'autore, non permette di sanzionare penalmente l'attività di chi, per esempio, scambi con un amico una copia di un software che entrambi hanno acquistato regolarmente, dato che il reato si manifesterebbe solo con l'utilizzo di detto software all'interno di un'attività produttiva (profitto), ovvero a seguito di cessione a titolo oneroso (lucro).
Questa interpretazione sarebbe giustificata dall'introduzione nell'ordinamento del prelievo fiscale che compensa gli autori e gli editori della cosiddetta copia privata, che deve pertanto essere considerata lecita.



>> Niente furto, niente ricettazione

Venendo a mancare il reato presupposto, appare altrettanto evidente l'insussistenza del conseguente reato di ricettazione. Ma c'è di più.
Pur accettando la tesi secondo la quale ci si troverebbe in ogni caso di fronte ad un reato previsto e punito dall'ordinamento, il software, il brano musicale e qualsiasi altra opera dell'ingegno resterebbero beni immateriali, come tali sottratti alla tutela incardinata dall'art. 648 c.p., il cui fine resta quello di non consentire la dispersione del denaro o altre cose di provenienza delittuosa.
L'esplicito riferimento della norma alle "cose", ossia a beni che hanno la caratteristica della "materialità", è di per sé sufficiente ad escludere qualsiasi riferimento alle opere dell'ingegno; né può servire a cambiare la sostanza il fatto che l'opera dell'ingegno sia incorporata su supporti ottici o magnetici, poiché questi ultimi, anche nel caso di duplicazione abusiva, sarebbero di provenienza lecita, configurandosi come copia privata.
Desta infine preoccupazione l'ipotesi di reato partorita in questi giorni da qualche Procura, secondo la quale anche il file sharing, ossia la condivisione di dati tramite reti telematiche, concretizzerebbe l'ipotesi di reato di ricettazione. I casi sono due: o sono cambiati i principi generali del diritto penale italiano (divieto di analogia e principio di legalità) e la modifica è passata inosservata ai più, oppure, com'è più probabile, qualcuno sta commettendo errori grossolani, e si rifiuta di approfondire il problema per motivi che non ci è dato conoscere.



Ciò che maggiormente sorprende e preoccupa, però, è la costanza e la perseveranza con la quale le Forze dell'Ordine e la Magistratura perseguono questi reati, che, benchè creino difficoltà alla nostra economia, hanno un effetto sulla collettività ben diverso dallo scippo, dalla rapina, dall'usura e da ogni altra attività che viene percepita dalla gente come un vero pericolo e un vero delitto.
E' evidente che il nostro ordinamento non rileva questa profonda differenza, nella speranza di tutelare penalmente interessi commerciali che, invece, trovano l'unica giusta collocazione sistematica e teorica nell'ambito del diritto civile.
Ma è altrettanto evidente che chiamare il 113 - magari in qualità di esperti di "associazioni senza fine di lucro che tutelano gli interessi di società con fine di lucro" - per indurre gli inquirenti a fare il lavoro che, in ambito civilistico, richiederebbe un avvocato ed una causa, costa certamente molto meno e rende molto di più dal punto di vista psicologico.
Se è vero che sarà difficile tornare indietro, speriamo, almeno, che lo stesso principio venga esteso agli inquilini che non pagano il canone di locazione (identico, per fine, al canone una tantum dovuto per la licenza d'uso), affinché i legittimi proprietari possano tornare in possesso dei loro immobili con una semplice telefonata alle Forze dell'Ordine.

Gianluca Pomante



L'ARTE

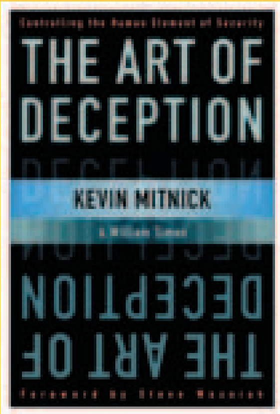
Si inventano nuove identità, riescono a ottenere informazioni riservate, entrano in posti a loro vietati: sono gli ingegneri sociali.

Chi vuole mettere in opera un piano d'attacco efficace a un sistema informatico, sfrutta in genere i bug del software, ma **anche i sistemi umani presentano le loro falle di funzionamento**, a volte ben più vulnerabili di quelle informatiche. La tecnica che sfrutta queste debolezze prende il nome di Ingegneria Sociale, o Social Engineering (SE). Di primo impatto, il termine Social Engineering potrebbe sembrare un termine innocente relativo alla sociologia, mascherando però i suoi scopi reconditi in campo informatico.

Con questo termine si indica in effetti l'insieme dei metodi e delle tecniche necessarie a **spacciarsi per qualcun altro**, qualcuno che ha diritto di accesso o di intervento su un sistema: il WebMaster di un sito, l'Admin di sistema o anche un semplice utente. **Significa principalmente saper mentire,** ed è una delle tecniche più efficaci utilizzate da chi si vuole introdurre in un sistema. L'unica che, se ben effettuata, non fallisce e non diventa obsoleta col tempo. Vengono sfruttati l'ingenuità o la scarsa professionalità altrui. Questa tecnica trova il suo massimo esponente in Kevin Mitnick, che ne fece un largo uso per le sue scorribande elettroniche (specialmente agli inizi della carriera).

Il S.E. è praticabile da chiunque, ma dall'abilità nel mascherarsi col volto di un'altra persona dipende un successo o una sconfitta. **Se fatto bene, può convincere chiunque**, anche un professionista del settore. Ed è proprio per questo che è estremamente pericoloso.

Lo scopo di questo articolo è mettere a fuoco le effettive potenzialità del S.E., permettendoci di **prendere coscienza dei rischi** e metterci in grado di **attuare un piano di contrattacco**. Viene scritto secondo ottica di un Admin che parla in terza persona spiegando il comportamento a cui si attiene un ipotetico attaccante.





Kevin Mitnick, alias il Condor, ha fatto del social engineering una delle sue armi principali durante le sue scorrerie informatiche. Scontata una pena (troppo) pesante, ha scritto un libro su come evitare di abboccare agli inganni.

DELL'INGANNO



>> Footprinting

La prima fase dell'attacco è quella del footprinting, cioè tutte quelle operazioni e tecniche che hanno come scopo **l'acquisizione di informazioni sul bersaglio**. L'attaccante cerca così di farsi un'idea precisa dell'ambiente che ha intenzione di colpire. Un tizio determinato può impegnarsi **anche per alcune settimane** in questa fase, a differenza del lamer che non la considera affatto. Questa fase gli permetterà di avere un'idea chiara sulla struttura aziendale e lo porterà ad effettuare un piano d'attacco di S.E., nonché gli sarà utile per acquisire quante più informazioni possibili, in quanto molte di queste gli potrebbero essere richieste.
Il footprinting viene attuato prima di qualsiasi attacco e non è quindi relativo al solo S.E.. Questo vuol dire che la ricerca di informazioni viene attuata anche per compiere successivamente un exploit.
Innanzitutto, se l'azienda o qualsiasi altra vittima ha un sito, **da questo si possono ricavare utili informazioni**. C'è da dire che spesso le aziende non realizzano e gestiscono in prima persona il loro sito Web, ma affidano questo compito a WebMaster o a società specializzate che sbrigano anche le pratiche burocratiche. In questo modo l'azienda non conosce i dati visibili dalla Rete e anche se questo aspetto viene sempre ignorato, si può rivelare estremamente pericoloso.
Può essere utile avere una copia del sito Web in questione sul proprio Hard Disk, avendo così una visione più chiara e precisa facilitando i processi di analisi (per esempio, Teleport Pro, www.teleport.com)

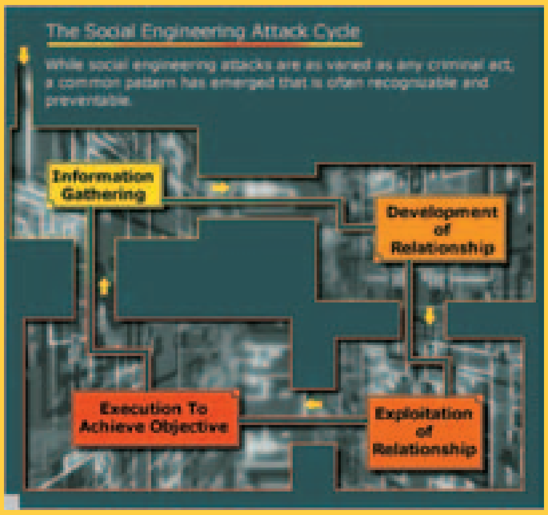
GLI STRUMENTI USATI

Questi i tool indispensabili al social engineer:

Due **telefoni**, uno fisso e uno mobile. Sarebbe anche utile disporre di un telefono pubblico sufficientemente isolato.
Uno **scanner**.
Una **stampante**.
Un **supporto cartaceo** per annotare tutte le info che acquisirà nella fase del footprinting.
Un **ambiente congruo**. L'attaccante cura al massimo tutti i dettagli spesso ritenuti secondari (es. non contatterà un'azienda dicendo di trovarsi in ufficio se in realtà chiama da casa mentre si odono gli schiamazzi dei cuginetti, né potrà dirlo stando nell'assoluto silenzio).

E se proprio fa sul serio, probabilmente userà anche:

Un **software** apposito per creare ed organizzare lo schema della struttura dell'azienda "vittima". Anche se inizialmente potrebbe apparire complicato, si dimostra invece facilmente utilizzabile mediante l'uso di PersonalBrain 2.1 Beta, molto adatto a questa esigenza. Il programma ha però due difetti: è basato su tecnologia proprietaria e funziona solo su piattaforma Windows.
Un **fax**.
Un **server di posta**. Dotarsi di un server SMTP sarebbe di estrema utilità all'attaccante in modo da poterlo riprogrammare a seconda dei casi (si consiglia SendMail).
Conoscenza dell'Inglese. Potrebbe tornare utile una conoscenza dell'Inglese che, in caso di utilizzo, dovrà essere ottima con un buon accento inglese (l'ideale sarebbe aver passato un certo periodo in Inghilterra).



Quattro fasi di un attacco basato sull'ingegneria sociale: raccolta di informazioni, sviluppo di relazioni, sfruttamento delle relazioni costruite per ottenere, esecuzione dell'attacco.

In ogni sito troveremo la sezione "**Contatti**". Da qui il social engineer solitamente troverà un contatto tecnico che potrà essere identificato in un soggetto operante nel settore assistenza (poi dipende anche dai casi e dal tipo di azienda). Troverà anche un contatto amministrativo.
Di entrambi di questi contatti troverà, quasi certamente, il **recapito telefonico**.
Dagli indirizzi e-mail potrà ricavare il **mail server**.
Nomi degli amministratori o delle principali figure di spicco ma anche ulteriori info potranno essere ricavati con alcuni piccoli software, come per esempio **Sombrero** (www.sombrero.it), che integrandosi con il browser mediante una semplice toolbar, fornisce informazioni preziose, anche se non sempre soddisfano le esigenze.



A volte potrebbe capitare che un'azienda pubblichi anche un **organigramma che illustri la struttura societaria**, manna dal cielo per l'attaccante.
Se ce ne sono, verranno sicuramente indicati nel sito i **partner commerciali dell'azienda**, sui quali l'attaccante ricercherà informazioni così come fa con l'azienda vittima.
Da una attenta analisi delle pagine Web, ricaverà i linguaggi Web usati e il programma usato. Ulteriori informazioni potrà avere leggendo scrupolosamente i tag di commento del sorgente della pagina.
Dovrà prestare attenzione anche a quelle immagini (se ce ne sono) che indicano il **tipo di server usato** e i modelli per la strutturazione del sito.
Attraverso il comando **Whois** offerto online dalle registration authority sarà possibile avere numerose informazioni tra i quali i nomi dei titolari del dominio, l'indirizzo IP, indirizzi IP dei DNS. I siti con dominio .it vengono gestiti dal Nic, i restanti sono quasi tutti gestiti da Internic o dal Ripe.



L'attaccante a questo punto farà **assidue ricerche** usando i motori del Web, leggendo e annotando tutte le informazioni disponibili sui contatti ricavati nelle precedenti fasi (un articolo su come usare i motori di ricerca lo trovate sul numero 24 di Hj). Si servirà di servizi che effettuano ricerche su più motori come **WebCrawler** (www.webcrawler.com) e **Profusion** (www.profusion.com) o utilizzerà appositi software come **Copernic**, **WebFerret** e **FirstStop WebSearch**. Sarà così accorto da controllare anche i **newsgroup**, i **forum** e le **mailing list** in quanto, a volte, gli amministratori e i WebMaster richiedono sui siti specializzati in sicurezza consigli o aiuti che, in un modo o nell'altro, possono rivelare proprio le loro debolezze. Questa fase termina qui, anche se le cose da dire sono così tante che si potrebbe andare avanti molto di più.

>> Scanning

È giunto il momento per l'attaccante di controllare se le informazioni fin qui raccolte sono attendibili o meno. In particolare, dovrà **verificare l'operatività degli indirizzi e-mail, dei recapiti telefonici e i contatti amministrativi**, in quanto molti siti potrebbero non essere aggiornati e quindi riportare informazioni ormai vecchie.







Proprio per questo fine, l'engineer chiamerà l'azienda ponendo domande del tipo: "Potrei cortesemente parlare con il Signor XXX? (dove per XXX sta il nome del contatto da verificare)". Se la risposta sarà del genere: "Il signor XXX non lavora più da noi", domanderà sul nome del sostituito. Una cosa simile si potrebbe fare via e-mail. Ovviamente tra una verifica e l'altra attenderà qualche giorno, poiché **una raffica di chiamate insospettirebbe l'azienda**.
Verificate le info ricavate, inizia il piano d'attacco. Probabilmente, l'attaccante seguirà scrupolosamente alcune regole generali riguardo al comportamento da adottare.

>> Comportamento

Un'idea per l'attaccante sarebbe quella di **studiare previamente lo "stile vocale"** della persona per la quale ha intenzione di spacciarsi (magari chiedendo pretestuosamente delle informazioni), evitando inflessioni dialettali e atteggiando la voce a un tono neutro e cortese. Tale studio del contesto in cui si muove la vittima è perciò ineludibile. È importante che l'ingegnere sociale sia un fine psicologo, nel senso che sappia innescare un moto di empatia anche per così dire "epidermico". È prioritario, all'interno di una ricostruzione dell'organizzazione del personale aziendale, focalizzare la posizione della figura professionale che viene contattata in relazione al personaggio che l'attaccante vuole interpretare, adattando relativamente il tono di voce. L'attaccante dovrà sembrare sciolto e naturale e atteggerà la sua voce a un tono neutro e cortese. Durante la pratica del piano d'attacco, avrà sempre vicino a sé e in maniera facilmente leggibile tutto ciò che è stato ricavato con il footprinting, dimostrandosi così sempre sicuro nel caso gli venga richiesta qualche informazione.

>> L'attacco vero e proprio

Dal sito dell'azienda ABC vengono ricavati tutti i contatti amministrativi, i relativi indirizzi e-mail e i contatti telefonici dell'azienda. Sempre dal sito si ricava che la sede della azienda è a Milano, ma una sua filiale è presente a Roma. Mediante alcuni motori di ricerca di cui abbiamo parlato nell'articolo, il cracker ricerca più informazioni possibili sulle persone di maggior spicco e scopre che l'Admin ha più volte chiesto in una mailing list aiuto riguardo la configurazione di un Apache 2.0 in quanto non aveva praticità con quel server. Tutte le informazioni vengono raccolte in PersonalBrain.
L'engineer telefona alla segretaria dell'azienda in cerca dell'Admin ma gli viene detto che questo si trova nella filiale a Roma e vi sarebbe rimasto per una settimana. Gli viene così passato il vice-Admin. Non interessa: riattacca. Da un'altra ricerca risulta che l'Admin gestisce anche un sito dedicato a una raccolta di spartiti musicali. Spacciandosi per un manager interessato all'acquisto del sito, il malintenzionato riceve una e-mail dall'admin con info.
Facendo il grabbing delle signature viene inviata un falso messaggio (con l'indirizzo e-mail dell'admin) al vice- admin nel quale si afferma che un tecnico verrà nella sede di Milano per la configurazione dell'Apache Server il giorno successivo. Si presenta il cracker il quale installa un trojan nel PC e si preoccupa di disattivare il firewall raccomandando l'aiuto admin di "non effettuare modifiche ai PC prima dell'arrivo dell'Admin"
L'attaccante è entrato nell'azienda, e ha preso controllo del server.

Leonardo Vaghaye 'Milo Cutty'
milo.cutty@libero.it

E C'È ANCHE CHI ROVISTA NELLA SPAZZATURA



Ok, fa schifo solo a pensarci, ma molti "ingegneri sociali" trovano gran parte delle informazioni riservate di un'azienda nella spazzatura: elenchi telefonici interni, liste di account, carta intestata, corrispondenza con clienti o fornitori, procedure interne... sono tutte cose molto preziose per chi vuol far credere di essere un dipendente dell'azienda, o comunque qualcuno legittimato a ottenere accesso a ulteriori informazioni. Sempre meglio quindi passare tutte le carte sensibili attraverso un tritadocumenti.



Prima delle console, prima delle schede grafiche accelerate per PC, prima ancora dei PC stessi, c'erano una volta i videogiochi da sala. Un progetto nato in Italia si propone di ridare vita a questi giochi, per farli conoscere ai più giovani, e far tornare giovani quelli ormai avanti con l'età.

Mame è un **emulatore di Console Arcade** che utilizzando il codice dei programmi arcade (le Rom) permette di **riportare in vita migliaia di vecchi videogiochi da Bar** (Coin Op) con una fedeltà al gioco originale, senza precedenti.

Il 24 dicembre 1996, Nicola Salmoria ha iniziato a lavorare su diversi emulatori (PacMan, Pengo, Crazy Climber, LadyBug e Rally X), che nel gennaio 1997 convergono in un solo programma che emula le diverse piattaforme Hardware ed ha bisogno solo delle Rom dei programmi per funzionare. A questo risultato viene attribuito il nome **Multiple Arcade Machine Emulator** (Emulatore di Molteplici Macchine da Videogioco), Mame.

La release ufficiale, Mame 0.01 vede la luce il 6 febbraio 1997 alle 00:32.

La filosofia di Mame è subito quella corretta: una piattaforma di sviluppo **Open Source** e una emulazione dell'Hardware basata su dei driver che vengono facilmente inseriti all'interno dell'eseguibile. La versione attuale è la 0.70b, che supporta 3990 ROM, per un totale di 2266 singoli giochi.

Le versioni di Mame non sono rilasciate in modo fisso, ma avvengono automaticamente ogni volta che si sono apportate un numero di modifiche sufficienti a giustificarne una nuova (miglioramenti dell'emulazione o incremento dei giochi supportati). Inizialmente l'attesa tra una versione e la successiva era di circa quattro mesi, mentre **ora l'intervallo si è ridotto a due o tre settimane**. Per i più irrequieti, è anche disponibile una pagina (Mame Work in Progess o WIP) da cui si può seguire l'andamento delle beta e tutte le modifiche che giorno dopo giorno porteranno all'uscita della versione successiva.

Il fine ultimo del progetto Mame è quello di **preservare tutte le schede prodotte per gli arcade negli ultimi trenta anni**. Attraverso Mame è stato possibile ripristinare delle schede che erano ormai morte da tempo a causa della rottura di alcuni componenti ormai introvabili o perché l'hardware necessario non era più disponibile sul mercato.

Attualmente fanno parte del team ufficiale di sviluppo **oltre 100 programmatori,** e Nicola Salmoria è ancora il coordinatore del progetto (oltre ad esserne uno dei maggiori contributori).



L'ARCHEOLOGIA DIGITALE



Nella storia di Mame svolge un ruolo molto importante anche un altro italiano, Mirko Buffoni, che però alla fine del 1988 abbandona il progetto principalmente per motivi di lavoro.

>> Cosa usare per Mame

Mame esiste in una infinità di formati. È possibile giocare a Mame con **Linux, Macintosh e ovviamente Windows**. Ma è anche possibile usarlo su **Windows CE, Amiga o sulle macchine fotografiche della Kodak**.
Il punto migliore da cui partire è il sito ufficiale di Mame,
www.Mame.net, ma per i neofiti la soluzione migliore è quella di scaricare **Mame32**, un progetto parallelo a quello di Mame, che unisce il motore di emulazione a una interfaccia grafica per Windows molto ben realizzata. Usando il semplice Mame, ci si trova solo di fronte ad un prompt senza sapere cosa fare, visto che il programma originale funziona solo da linea di comando.
Una volta scaricato il SW (se scegliete Mame32 sarà necessario anche registrarli sul sito di Planetshare per eseguire il Dowload) vi servono le Rom.
Se Mame è il corpo del progetto, **le Rom sono la sua intelligenza**. Le Rom sono le immagini dei dati di tutti quei chippetti che popolavano le schede dei vecchi Coin Op. Le dimensioni delle Rom variano da **pochi KB fino a oltre trenta Megabyte**! (nelle ultime versioni è stato aggiunto anche il supporto per le immagini dei dischi rigidi presenti negli arcade di ultima generazione, i file .CHD, che arrivano a oltre un Gigabyte!).

MAME SULLA MACCHINA FOTOGRAFICA



Qualcuno si è preso la briga di fare uno dei porting più improbabili di Mame: ne ha realizzato una versione per le fotocamere digitali Kodak! In questo modo può giocare anche in vacanza, tra uno scatto e l'altro. Per saperne di più, visitate il sito http://digita.Mame.net.

Per iniziare subito (legalmente) a giocare, tutto quello che dovete fare è andare nella sezione Download del sito ufficiale, e scaricare uno dei (tre) giochi che gli autori hanno deciso di distribuire gratuitamente. Una volta scaricate le Rom necessarie, quasi sempre in un unico file zip, è sufficiente **copiare il file zip nella directory "rom"** dell'emulatore e lanciare Mame. Al primo avvio, gli emulatori possono essere molto lenti, visto che devono eseguire una miriade di controlli. Dal secondo avvio in poi, la velocità di caricamento diventerà accettabile.
Giocare è facile: con il tasto **5** si aggiungono le monetine, i tasti **1** e **2** permettono di selezionare la partita per

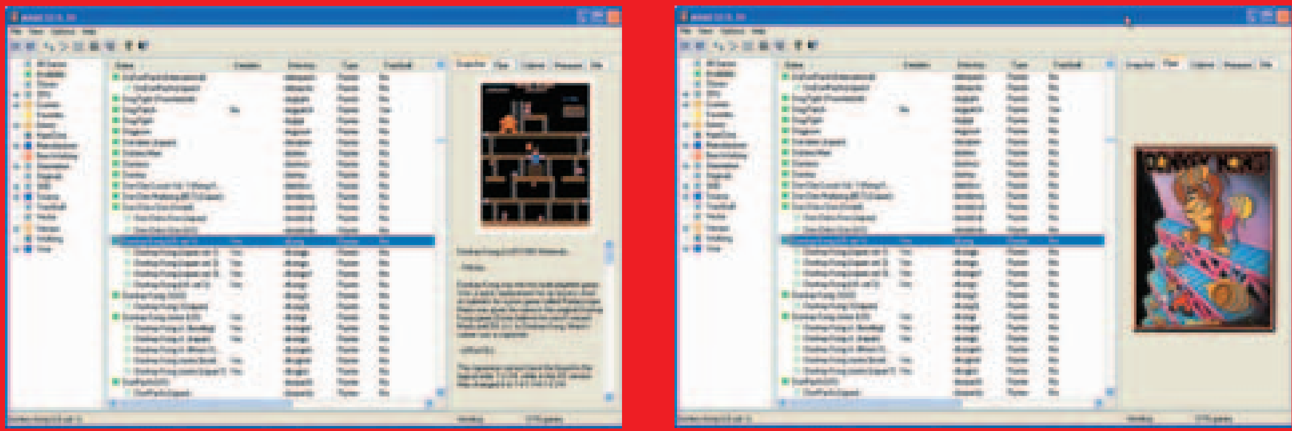
COSTRUIAMO IL NOSTRO CABINET

Sul prossimo numero spiegheremo come costruire un cabinet arcade con



pezzi che si possono recuperare in giro. Quella appoggiata sulla sedia è una scheda originale di street Fighters II! Notate che il cabinet funziona con monete da 200 lire.
Se volete saperne subito di più, potete visitare i siti Build Your Own Cabinet (www.arcadecontrols.com/arcade.htm), Zelig game Machinez (in italiano, www.geocities.com/SiliconValley/Peaks/8233/index2.htm) o J-Pac (www.ultimarc.com)





Mame 32 è la migliore soluzione per iniziare ad usare subito Mame su Windows. Deriva direttamente dal progetto originale, è perfettamente integrato con un proprio front end che gestisce i giochi, vi mostra le informazioni e le immagini e tiene conto delle statistiche dei giochi più usati. Inoltre, permette di vedere le Rom ordinate in vario modo, raggruppando informazioni interessanti come la versione di Mame in cui il gioco è stato inserito, il genere oppure la casa produttrice. Nella foto utilizza anche il file HISTORY.DAT con informazioni e curiosità sul gioco selezionato.

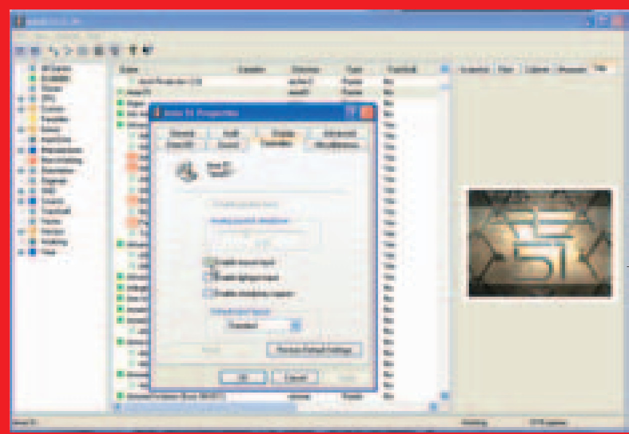
uno o due giocatori, **le frecce** sono le direzioni del joystick, il tasto **control** permette di sparare assieme alla **barra spaziatrice** (comunque la configurazione dei tasti è modificabile per ogni singolo gioco, in modo da venire incontro alle esigenze di qualsiasi utente). Se dovete andare al bagno a metà partita premendo **P** potrete sospendere il gioco per riprenderlo quando vorrete (quante volte avete desiderato di poterlo fare in sala giochi…).
Una interfaccia semplice ed intuitiva che è da sempre stata alla base del successo di Mame.

>> Scavando nelle impostazioni

Le funzioni che l'emulatore mette a disposizione sono comunque molte di più. Per esempio, c'è la possibilità di eseguire una **copia del video**, o **salvare una partita** interrotta. Divertente anche l'opzione **DipSwitch** che vi fa vedere tutte le possibilità che venivano lasciate al barista: **3/4/5 omini, gioco facile/difficile, bonus level sì/no, nuova vita a 10000/20000/50000 punti…** Ecco forse perché il vostro amico con la stessa macchina in un altro bar aveva la vita più facile…
Un suggerimento: cercate di apprezzare Mame soprattutto per i vecchi arcade. Le sue performance nei giochi dopo il 1995/96 sono abbastanza scarse, anche usando un computer potente. Immaginate che nel mio Cabinet Arcade uso AdvenceMame 0.64 con un P2 400MHz e 192 MB di Ram, mentre per giocare ad Area 51 (1995 con una immagine CHD di 534MB) è consigliabile un P4 da almeno 3GHz.
Si vocifera che sia in preparazione una versione di Mame che utilizzerà **l'accelerazione hardware** delle moderne schede video, ma credo che il lavoro fin qui svolto sia più che sufficiente e che avvicinarsi troppo ai giorni attuali con l'emulazione può attirare troppo l'attenzione di chi con i video giochi ci lavora davvero, vedendo in Mame **non un piacevole passatempo ma un nemico che gli porta via il pane di bocca**.

>> Mame, le Rom e la legge

Purtroppo non ci sono dubbi: **avere una collezione di Rom è un reato punto.**
Alcuni siti permettono di scaricare le ROM, avvertendo che è possibile provarle per 24 ore, dopodiché devono essere cancellate dal proprio disco fisso: **sono tutte balle!** Il solo atto di scaricare una Rom non è consentito. L'aspetto legale del problema finisce qui, però bisogna anche dire una cosa a sostegno di Mame. Moltissimi dei giochi che sono emulati sul sistema, **senza il progetto Mame sarebbero da molto tempo caduti nel dimenticatoio**, e le stesse case di produzione (a dire il vero molto poche) che si lamentano della pirateria delle Rom per Mame, **senza Mame si ritroverebbero adesso senza oggetto del contendere**.
Mame è l'oggetto che a distanza di an-

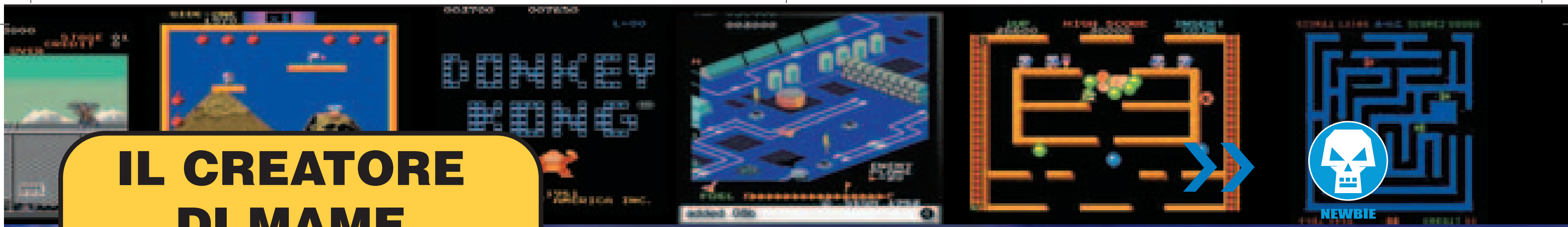


Alcuni giochi come Area51 richiedono una pistola Laser. Al suo posto, potrete usare il mouse configurando l'opzione Controllers delle proprietà del singolo gioco. È possibile anche abilitare il Joystick, anche in versione Usb.

I LINK PIÙ IMPORTANTI

Per chi ha fretta, ecco alcuni tra i siti su Mame più importanti. Chi vuole saperne ancora di più, troverà nella sezione Contenuti Extra della Secret Zone di hackerjournal.it, una trentina di siti e pagine selezionate dalla redazione.

Mame:
Mame (ufficiale)
www.Mame.net
Mame32
www.classicgaming.com/Mame32qa/
HighScores
www.Mameworld.net/highscore/
Madda's Mame (in italiano)
http://web.tiscali.it/no-redirect-tiscali/velmadda/Index.htm
Emuita (in italiano)
www.emuita.it



NEWBIE

IL CREATORE DI MAME

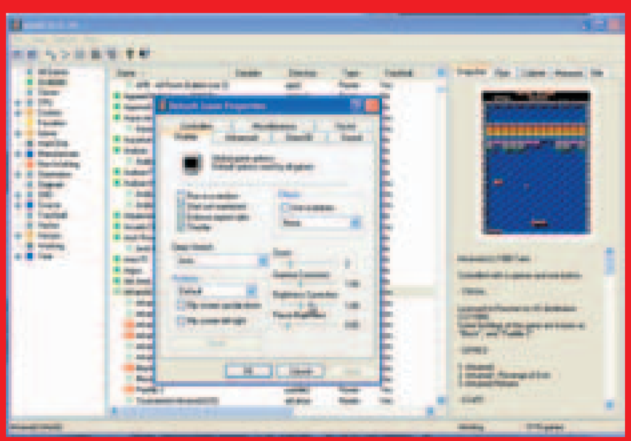
Nicola Salmoria ha 33 anni e si è da qualche mese laureato in Matematica presso l'università di Siena con la votazione di 110 e lode.
La sua tesi di laurea dal titolo "il progetto Mame: reverse engineering e macchine da gioco" è senza ombra di dubbio il manifesto di Mame e vi suggerisco di leggerla (la trovate su www.Mame.net/tesi.pdf).
Se volete sapere qualcosa in più di Nicola Salmoria, la cosa migliore da fare è chiedergliela di persona sul newsgroup it.comp.software.emulatori, oppure leggersi l'intervista pubblicata all'indirizzo www.emuita.it/spider.php?pagina=intervista&id=15).
L'intervista è molto interessante, per esempio si scopre che Nicola non è stato un grande frequentatore delle sale giochi (giocava a Pac Man, a Moon Patrol, Lady Bug, ma moriva subito).
Per Nicola, il progetto Mame è stato una sorta di rinascita personale: dopo anni di Amiga, Nicola era da poco passato al PC, senza però trovare stimoli alla programmazione. Alla vigilia di Natale del 1996, gli è capitato tra le mani il codice sorgente di Pac Man, ed è nata una sfida: portarlo sul PC così com'era.

ni ha dato nuovamente valore a quelle Rom; senza Mame non si sarebbe probabilmente scatenata quella corsa all'hardware retrò che su eBay fa valere un **vecchio cabinet DonkeyKong 900 Dollari**, o una Vetrofania di PacMan (Marquee, ovvero la scritta illuminata in cima ad ogni arcade) **anche 100 dollari!**
Molte case di produzione non esistono più, ma se i loro diritti per i prossimi 70 anni restano validi ed alla fine potrebbe sempre spuntare fuori qualcuno che per legge ne ha la proprietà.
Attualmente esistono solo tre giochi per i quali i proprietari hanno ufficialmente rinunciato ai diritti: **Gridlee, Poly-Play e Robby Rot.**
Se nonostante tutto volete collezionare Rom, i programmi indispensabili per mettere in ordine e certificare la collezione sono **Clear Mame Pro** (il migliore gestore di Rom disponibile), seguito a ruota da **MameMerge**.

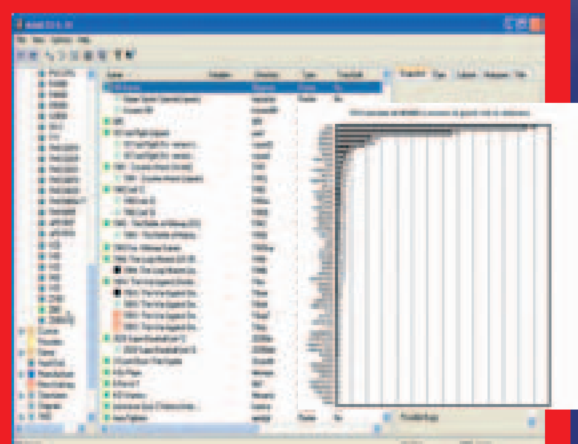
» L'aiuto dei non programmatori

Non serve essere un brillante programmatore C per partecipare alla comunità Mame. Molti progetti importanti che supportano Mame sono stati elaborati da persone che non sono programmatori. Tra i progetti più interessanti è da segnalare il contributo di Martin Pugh (Pugsy) da una piccola città del Galles e quello di Alexis Bousiges che gestiscono rispettivamente la **lista di tutti i cheat (trucchi) e la storia di ogni singolo videogioco emulato**.
Indispensabili sono anche i contributi di chi ha raccolto e catalogato **le foto dei cabinet nelle sale giochi**, chi con infinita pazienza ha trovato e scannerizzato i depliant pubblicitari (flyers) dei giochi. Altri si sono dedicati ai **marquee**.
Leezer (leezer@leezer.karoo.co.uk) gestisce il file HighScore, in modo non ufficiale, raccogliendo in giro per la Rete **i punteggi più alti totalizzati dai vari giocatori.** Se amate la sfida dovete assolutamente scaricare il file e cercare di battere il punteggio migliore nel vostro videogioco preferito! Senza il loro aiuto, il progetto avrebbe mancato di un collegamento alla realtà e di quel rigore che Nicola Salmoria voleva quando ha scritto **"I videogiochi arcade costituiscono un'importante parte della nostra cultura popolare che rischia di andare perduta a causa dell'obsolescenza dell'hardware**. Nell'ottica della conservazione e della trasmissione alle generazioni future di un prodotto della creatività umana, è ampiamente motivata un'opera di recupero, archiviazione e documentazione. Con pertinente analogia, chi si dedica a tale opera è una sorta di archeologo, un **"archeologo digitale"**, per citare l'appropriata definizione, alla quale sono piuttosto affezionato, coniata tempo fa da un giornalista"
Certamente è anche grazie a questa serie di appassionati che dedicano il loro tempo libero alle ricerche delle informazioni, che il progetto Mame ha avuto un così grande successo ed è destinato a mantenerlo per ancora un lungo periodo.
Una ultima avvertenza agli esterofili: Mame si pronuncia Mame (all'italiana) e non "meim"…

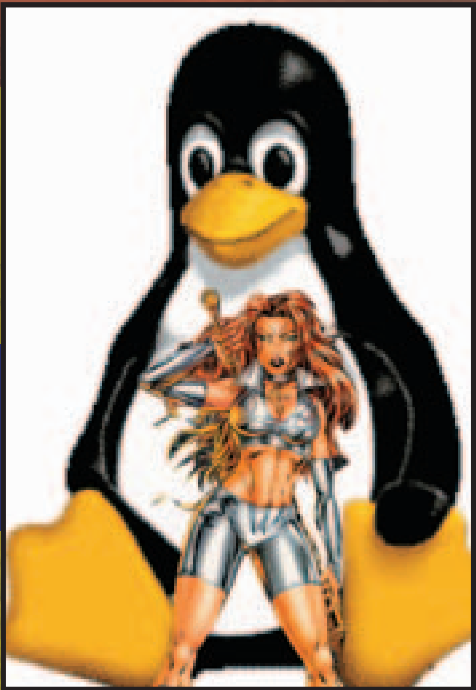
Guglielmo Cancelli e SpeedyNT



Utili le opzioni di Mame32 che permettono di cambiare la luminosità del quadro. Queste funzioni, come anche il controllo del volume, sono disponibili anche durante la partita.



Ecco le CPU più usate nell'emulatore Mame. Spicca lo Z80 che tra gioco (1240) e audio è sfruttato da 2493 giochi.



LINUX SENZA INSTALLAZIONE

Volete provare Linux ma siete atterriti dall'idea di partizionare l'hard disk, di perdere dati, o di non saper tornare a Windows? Con una distribuzione "Live", che parte dal CD, passa tutta la paura!

Immaginate di trovarvi in un laboratorio informatico, o in un cybercafé, o ancora a casa di un amico e di poter **ricreare in pochi minuti su questo computer a voi sconosciuto un ambiente attrezzato e configurato per le vostre esigenze**. Non sarebbe fantastico? Bene, è possibile. Basta inserire un cd nel lettore e riavviare per essere subito operativi. Il tutto grazie alle recenti e particolari **versioni di Linux su CD-ROM, già pronte per l'uso senza dover installare nulla.**

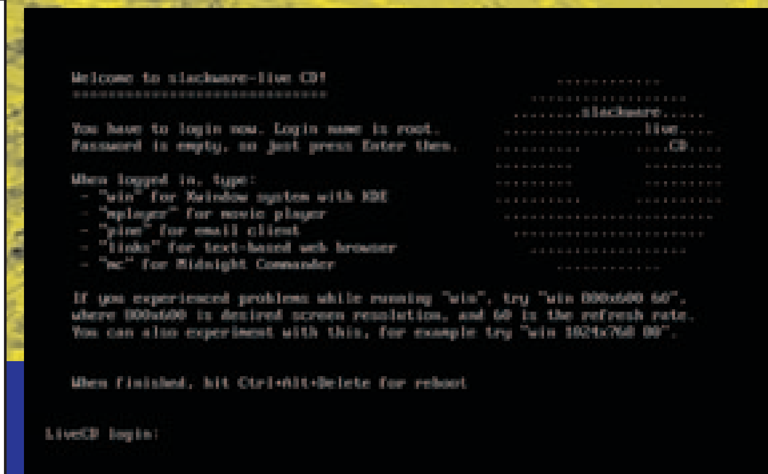
>> Un po' di storia: tiny distros e live CD

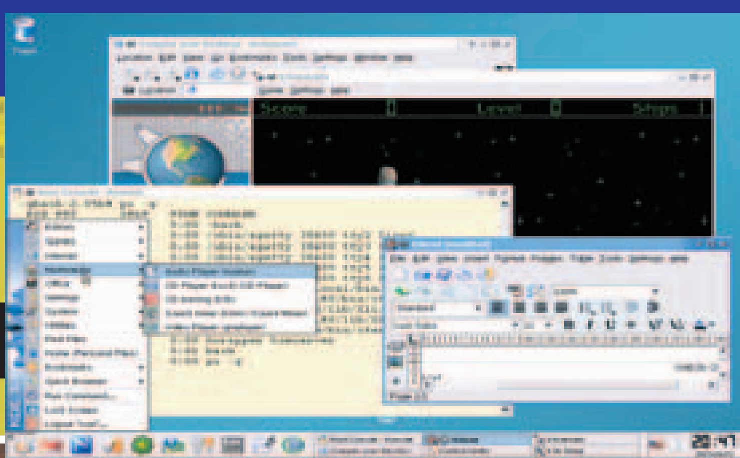
Le distribuzioni Linux su CD non nascono dal nulla ma sono il **logico proseguimento di una categoria molto particolare di versioni dette minimaliste, o "tiny"** (http://dmoz.org/Computers/Software/Operating_Systems/Linux/Distributions/Tiny), cioè minuscole.

Nel corso degli anni tra le numerose decine di distribuzioni ne sono nate diverse dalla grandezza ridotta: alcune sono pensate per sistemi embedded, altre funzionano da semplici directory e sono avviabili direttamente da Ms-Dos o Windows, altre sono addirittura "compresse" su un solo dischetto, come il pratico e compatto sistema-router **Freesco** (www.freesco.org).

Tuttavia questi Linux sono spesso il prodotto di un "hack": offrono solo un set specializzato (e quindi limitato) di funzionalità e richiedono spesso conoscenze tecniche e tempo a disposizione per essere installate, configurate ed usate.

Ecco dunque che, più di recente, sono comparsi **i "Live CD": versioni complete** (o comunque molto ben dotate) di **Linux, inclusive anche di interfaccia grafica, avviabili ed adoperabili da CD senza installare nulla**. Uno strumento pratico (e molto furbo aggiungerei) per permettere all'utente Windows indeciso (www.livingwithoutmicrosoft.org/article.php?sid=114) o almeno curioso di dare una buona sbirciata al sistema operativo del pinguino prima della rituale e sempre trau-





NEWBIE

matica formattazione e creazione di partizioni.
I principali nomi che offrono "live CD" sono le storiche **Slackware** (che ha diffuso di recente una versione con l'ultimo ambiente grafico KDE) e Debian, la francese **DemoLinux** (www.demolinux.org) e **GenToo** (questa e Debian anche per le piattaforme RISC PowerPC) o la commerciale SuSE.

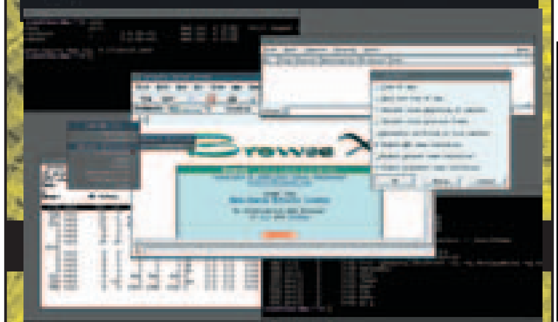
>> Ma non sono i soli

A dire il vero **i sistemi Linux non sono gli unici a poter essere eseguiti direttamente da CD**. L'**OS/2** della IBM, il **Mac OS** di Apple o ancora l'indimenticato **Be OS** (che sta ora rinascendo con il nome "Zeta" sviluppato dalla YellowTab www.yellowtab.com), permettono non solo di avviare ma persino di **creare setup personalizzati per riavviare la macchina in caso di problemi, ripristinare le postazioni di un laboratorio o ricreare un proprio ambiente di lavoro ovunque.** Tutte **motivazioni che i sistemi Linux su CD condividono, con in più il vantaggio di essere a costo zero**. Perciò, laddove realizzare un cd avviabile con Windows (www.nu2.nu/bootcd/) è laborioso e problematico, nonché funziona solo su alcune versioni (www.heise.de/ct/english/99/11/206/), la **modularità e flessibilità dei sistemi GNU-Linux,** creati da smanettoni per gli smanettoni, ha fatto fiorire una miriade di iniziative, nate anche grazie alle preziose informazioni disponibili su siti come Linux From Scratch (www.at.linuxfromscratch.org).

>> Cosa offrono i Linux su CD

Per descrivere o anche solo elencare il cosmo variegato e mutevole di distribuzioni disponibili sarebbe necessario occupare diverse pagine, perciò in questa sede ci limiteremo ad una concisa selezione di quanto è possibile scaricare e masterizzare e rimandiamo alle coordinate negli approfondimenti a fine articolo.
Attualmente lo scettro di versione più popolare, nonché apprezzata dagli smanettoni (che hanno basato i loro Linux su di essa), appartiene a **Knoppix** (www.knoppix.com), creata da un ingegnere tedesco, Klaus Knopper, che è riuscito nell'intento che si prefiggeva: realizzare "un sistema denso di funzioni per dimostrazioni ed emergenze su un unico CD, che inoltre solleva l'utente dal compito di identificare l'hardware, configurare i driver, periferiche e l'interfaccia grafica". Altri sistemi si specializzano invece ad esempio nella diagnostica e riparazione dei computer. È questo il caso di SuperRescue (www.kernel.org/pub/dist/super rescue) o di Trinity Rescue Kit (http://trinityhome.org/trk/), basata su Mandrake 9.0 o di incredibili sforzi di ottimizzazione come i progetti Bootable Business Card LinuxCare BBC (www.linuxcare.com/bootable_cd) e





LNX-BBC (www.lnx-bbc.org), pensate per entrare nel formato ridotto dei cd a forma di carta di credito (come dicono anche i nomi stessi). Ancora più notevole è la distro RepairLix (http://sourceforge.net/projects/repairlix/) che di mega ne occupa solo 12. Altrettanto compatte sono **Damn Small Linux** (www.damnsmalllinux.org), che con i suoi 50 megabyte occupati entra anch'essa su una cd-card, o lo scattante **Freedom OS** (www.softkits.com/Freeloader). Non meno interessante è l'italianissima **dyne:bolic** (http://dynebolic.org), **concepita come sistema multimediale e utilizzabile come tool di produzione audio/video.** Con questa versione di Linux oltre a scrivere, fare navigazione, elaborare immagini è possibile remixare, modificare, convertire, codificare audio e video, nonché fare streaming (come mostrato nell'edizione dello scorso anno della manifestazione Hackmeeting). Tornando in ambito più tecnico un altro utilizzo è naturalmente quello come strumento per effettuare analisi di rete. Linux è un sistema dall'ampio parco applicativi in questo ambito (pensiamo ad Ethereal) e un vantaggio della soluzione su CD, oltre a permettere di essere operativi ovunque e in pochissimo tempo, è la non-modificabilità permanente del sistema (in quanto su sistema a sola lettura)



Nicola D'Agostino
dagostino@nezmar.com



LE USA ANCHE LA SCIENTIFICA!

Le distribuzioni Live vengono usate spesso anche per indagini criminali, come consigliato anche in un recente workshop su questa tematica al Webbit di quest'anno (www.webb.it/event/eventview/893/). Per effettuare perizie, magari su macchine compromesse o su computer sequestrati durante casi di dibattimento processuale, sembra ad esempio ideale la distribuzione Fire (http://biatchux.dmzs.com/), che fornisce un ambiente specializzato. Sia sotto ambiente grafico che in quello testuale Fire ha già installati diversi strumenti per svolgere attività come analisi forense, recupero dati, scansione antivirus, test di vulnerabilità e altro ancora. Con le distribuzioni Live specializzate in analisi forensi si evita qualsiasi modifica al contenuto dell'hard disk, che costituisce la prova: così facendo, non è possibile cancellare delle prove per sbaglio, o per colpa di qualche bomba logica inserita dall'indagato.

IL TUNNEL

Probabilmente vi sarà capitato di aver letto, durante le vostre peregrinazioni tra forum, chat e siti ad argomento sicurezza, l'espressione "tunneling http". In quest'articolo cercheremo di spiegarvi l'http tunneling sia da un punto di vista teorico che con un esempio pratico che svolgeremo insieme.

>> Perché nasce

Il tunneling http nasce dall'esigenza di **poter utilizzare applicazioni che viaggiano su porte diverse dalla 80** in reti protette da firewall in cui l'unico accesso all'esterno è un proxy server per il web http e https(443). Il tunneling viene quindi utilizzato da quegli utenti di reti aziendali e simili che, non tollerando che l'amministratore di sistema impedisca loro di utilizzare WinMx & C bloccandone le porte, **utilizzano un tunnel http per dirottare le sessioni del loro p2p sulla porta 80**. Un tunnel è infatti una piccola applicazione che, come indica il suo nome, crea una via diretta tra due sistemi spostando la comunicazione da una porta ad un'altra.

>> Esempio pratico

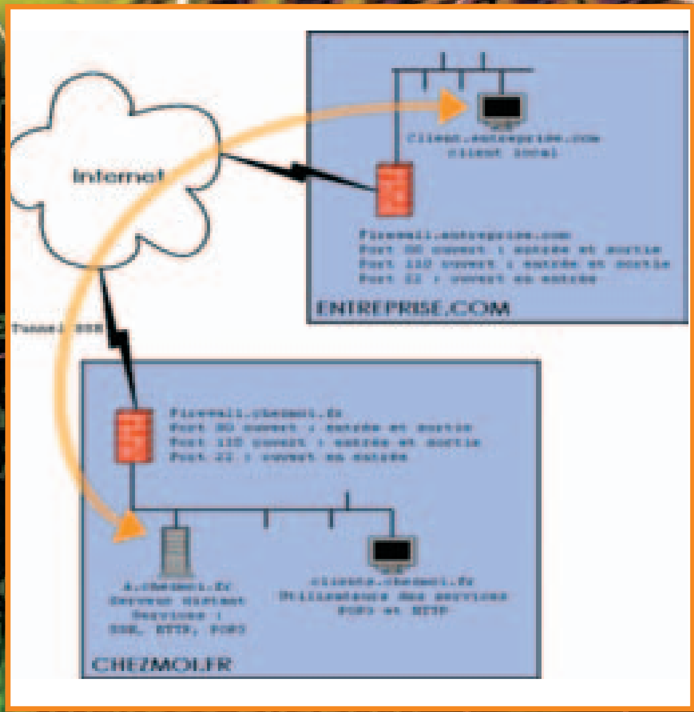
Per farvi comprendere meglio quanto detto passiamo subito ad un esempio pratico. Scaricate all'indirizzo indicato nell'area link l'**http tunnel di Alex Turc su Code Project**. Naturalmente non è un tunnel professionale ma è perfetto per i nostri scopi. Inoltre è possibile scaricare anche il sorgente in C++.

All'interno del file zip troverete un eseguibile (**HTTPTunneling.exe**) e un file di testo con estensione .cfg (**HTTPTunneling.cfg**). Se aprite con notepad il file di configurazione vi troverete di fronte la seguente intestazione:

```
# HTTP tunneling configuration file
# Application is developed by Alex Turc ( alex_turc@hotmail.com; alex@cs.ubbcluj.ro )

#-----------------------------------------------------
#Source port    Destination address   Destination port  Proxy address   Proxy port
#-----------------------------------------------------
     80           192.168.0.2                21
```

NELLA RAGNATELA



Nel primo campo **Source port** va indicata la porta su cui ascolterà il Tunnel (nel nostro esempio la porta 80); nei campi **Destination address** e **Destination port** deve essere indicata l'indirizzo e la porta su cui deve dirottarci il tunnel (nel nostro caso la porta FTP di 192.168.0.2); nei campi **Proxy address** e **Proxy port** è possibile indicare un proxy che il tunnel dovrà utilizzare per arrivare a destinazione. L'esempio che vi esporrò è stato realizzato su tre computer in rete di cui uno fa da client, su un altro è installato il tunnel e l'ultimo fa da server di destinazione (con installato Windows 2000 Server).

Una volta configurato il file HTTPTunneling.cfg con i dati del server di destinazione, facciamo partire il file HTTPTunneling.exe che deve trovarsi nella stessa cartella del .cfg. **Apparentemente non succede niente**, se avete un firewall installato vi avvertirà che l'applicazione HTTPTunneling.exe sta cercando di aprire la porta 80 in ascolto e di operare come server. In tutti i casi se aprite il task manager troverete l'HTTPTunneling.exe tra i processi e da lì **potrete eventualmente terminarlo**.

Se adesso, da un altro computer, provate a effettuare un collegamento con telnet sulla porta 80 del computer con installato il tunnel, **vi risponderà direttamente il server** (FTP nel nostro caso) di destinazione. Da questo piccolo esempio capite come sia possibile, per chi si trova all'interno di una rete protetta da firewall, **potere utilizzare qualunque applicativo facendolo passare attraverso la porta 80**. Sempre infatti rimanendo nel caso del server FTP, una connessione diretta non sarebbe permessa dal momento che opererebbe sulla porta 21 cui è preclusa l'uscita. Se però **installiamo il tunnel sul nostro computer di casa collegato a internet con un ip identificabile**, siamo in grado dall'ufficio, collegandoci alla porta 80 del nostro computer di casa, di aggirare le politiche di sicurezza della nostra azienda.

http Tunneling su linux



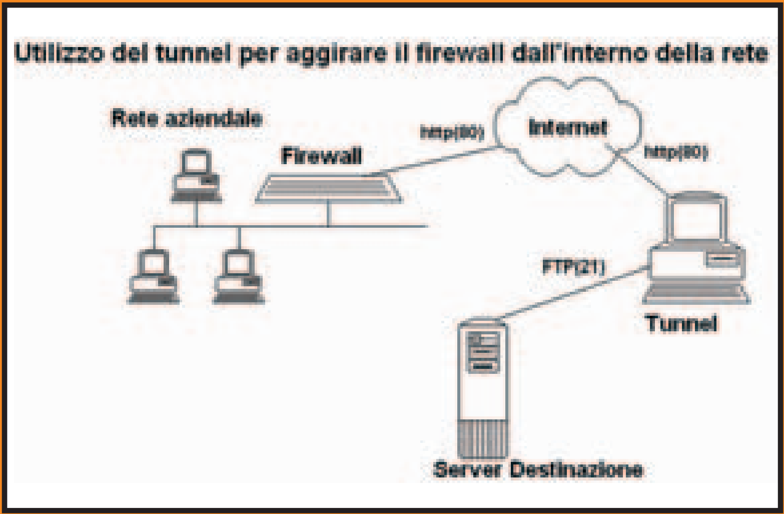
Per implementare il tunneling nel sistema operativo del pinguino esiste un applicativo sviluppato e mantenuto da Lars Brinkhoff. È un software libero distribuito con licenza GNU GPL. L'indirizzo da cui scaricarlo lo trovate tra i links. Vi trovate anche delle FAQ sull'http tunneling in inglese.

>> Spesso è meglio non usarlo

Inutile dire che una pratica di questo tipo è altamente sconsigliata. Le politiche di sicurezza di un'azienda **esistono per un motivo ben preciso** e non soltanto a tutela dell'azienda stessa ma **anche dell'utente**. Per esempio, spesso nelle reti aziendali viene centralizzato lo scaricamento della posta che poi viene ridistribuita ai client; viene evitato insomma un contatto diretto tra server di posta esterno all'azienda e client. Ciò a volte avviene per far sì che il controllo su virus e amenità varie che arrivano con la posta sia centralizzato sul server per questioni di praticità: si scaricano una sola volta gli aggiornamenti sui virus, il carico elaborativo pesa sul server che è in genere una macchina con più risorse, il client viene esentato da questo compito a volte molto oneroso da un punto di vista elaborativo. Inutile dire che **utilizzare un tunnel che ci diròtti su un server di posta esterno attraverso la porta 80 manderebbe tutto a monte**.

>> Altri problemi di sicurezza

Rimanendo sempre nell'esempio fatto in precedenza, pensate che il tunnel che abbiamo utilizzato non soltanto **non autentica in ingresso, ma non logga neanche**! Nonostante infatti un file di log venga creato(HTTPTunneling.log) non sono collezionate informazioni relative agli ip di provenienza e ciò significa che,





qualora qualcuno scopra che sul nostro computer di casa c'è un tunnel, **potrebbe utilizzarlo come anonimizzatore per azioni dirette al computer che noi abbiamo indicato essere la destinazione del tunneling**. Se poi riuscisse a modificare il file .cfg il vostro computer potrebbe essere utilizzato come anonimizzatore **per tutte le destinazioni**.
Fatte queste doverose precisazioni sull'utilizzo 'canonico' del tunneling, esistono innumerevoli casistiche in cui il tunnel **può essere utilizzato come strumento d'attacco**. Una per tutte: il caso di un server interno che accetta accessi soltanto da un certo range di ip. A parte lo spoofing, l'installazione di un tunnel su una macchina vulnerabile della rete **potrebbe consentire l'accesso a server di questo tipo** aggirando anche l'eventuale firewall.

>> Andiamo nel dettaglio

Per vedere nel dettaglio il funzionamento del nostro tunnel utilizzeremo **windump** (la versione per Windows di **tcpdump** per linux), avviandolo sul computer con il tunnel attivo. Ecco un estratto dell'output di un esempio che abbiamo fatto in una rete configurata come specificato sopra:

```
18:23:23.427174 IP PORTDECODER.3974 > DECODER.80: S 29402177:29402177(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
18:23:23.427317 IP DECODER.80 > PORTDECODER.3974: S 1436954387:1436954387(0) ack 29402178 win 17520 <mss 1460,nop,nop,sackOK> (DF)
18:23:23.427770 IP PORTDECODER.3974 > DECODER.80: . ack 1 win 8760 (DF)
18:23:23.443239 arp who-has DECODER-SERVER tell DECODER
18:23:23.443444 arp reply DECODER-SERVER is-at 0:50:ba:ce:7d:5e
18:23:23.443492 IP DECODER.1571 > DECODER-SERVER.21: S 1437016455:1437016455(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
18:23:23.443708 IP DECODER-SERVER.21 > DECODER.1571: S 1476348099:1476348099(0) ack 1437016456 win 17520 <mss 1460,nop,nop,sackOK> (DF)
18:23:23.443781 IP DECODER.1571 > DECODER-SERVER.21: . ack 1 win 17520 (DF)
```

Le prime tre righe dell'output di windump fanno riferimento al momento iniziale cioè alla connessione TCP che avviene tra il client **PORTDECODER** ed il tunnel **DECODER**. Come potete notare la connessione avviene sulla porta 80 con il classico handshake SYN-SYN/ACK-ACK. Subito dopo il tunnel **DECODER** ricerca la destinazione. Nel caso allo studio, il server di destinazione si trova all'interno della stessa sottorete, perciò è sufficiente un'interrogazione arp cui segue la restituzione del MAC addresss di **DECODER-SERVER**. Le tre righe successive sono relative alla connessione TCP tra il tunnel (**DECODER**) e il server (**DECODER-SERVER**) sulla porta 21 dell'FTP. La sessione avviata viene registrata anche nel file di log del tunnel in questo modo:

```
Fri Jun 13 18:23:23 2003      Information     Direct tunnel request. Destination 192.168.0.2:21.
Fri Jun 13 18:23:23 2003      Information     Direct tunnel 0X00EB365B constructed. Destination 192.168.0.2:21
Fri Jun 13 18:23:48 2003      Information     Tunnel 0X00EB365B removed.
```

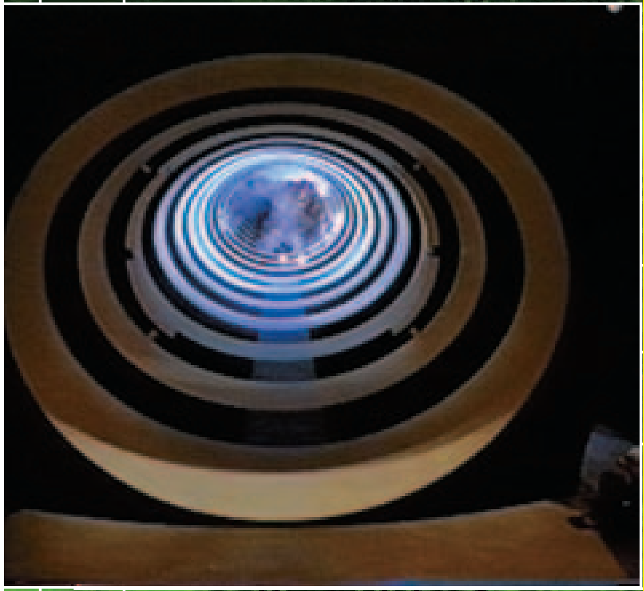
Come potete vedere voi stessi, le informazioni registrate sono relative **esclusivamente all'istante di creazione e distruzione del tunnel ed alla destinazione** (192.168.0.2 è l'ip di DECODER-SERVER). Il tunnel creato è caratterizzato da un identificativo (**0X00EB365B**): questo è tipico delle applicazioni a thread e consente l'apertura di più sessioni contemporaneamente sulla stessa porta (come praticamente avviene per tutti i servizi di rete).

Unico neo di questo piccolo ma funzionale tunnel, è la **mancata gestione dell'autenticazione sui proxy** perciò se volete utilizzare dei proxy d'appoggio da inserire nel file di configurazione, dovreste trovarne uno aperto.

>> Conclusioni

Concludiamo questo articolo con qualche considerazione rivolta agli amministratori di sistema di reti aziendali. Dal momento che il tunnel come abbiamo visto non viene installato all'interno della rete, l'unico modo per verificarne il suo utilizzo da parte di qualche vostro utente sarebbe **l'analisi dei pacchetti passanti attraverso le porte consentite**. Naturalmente questa è una soluzione abbastanza improponibile, oltreché lesiva della privacy dei dipendenti, perciò un'alternativa può essere l'utilizzo, sul proxy interno, di **applicativi che limitino il traffico di ogni sessione** per evitare almeno l'utilizzo di programmi di file sharing. Un ultimo appunto che spero non venga frainteso: spesso i tunnel, come quello del nostro esempio, non vengono rilevati dagli antivirus. ;-)

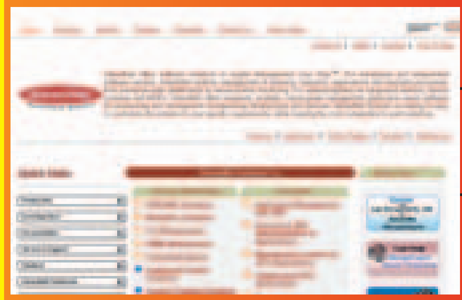
Roberto "dec0der" Enea
decoder@hackerjournal.it



Link utili



http://www.codeproject.com/internet/httptunneling.asp
Il link da cui scaricare l'http tunnel ed il suo codice sorgente



http://www.adventnet.com/products/snmp/help/developer_guide/sasapi/appletapi_http.html
Utilizzo degli applet java attraverso l'http tunneling



http://www.nocrew.org/software/httptunnel.html
http tunnel per Linux



http://www.http-tunnel.com
Soluzioni professionali di http tunneling